Entity Reference

/ Amster 7.0.2

Latest update: 7.0.2

ForgeRock AS.
201 Mission St., Suite 2900
San Francisco, CA 94105, USA
+1 415-599-1100 (US)
www.forgerock.com

Abstract

Reference of the ForgeRock® Access Management command-line interface entities.

Table of Contents

Overview

This reference contains:

- Entities supported in Amster commands
- Actions you can perform with Amster commands.

About ForgeRock Identity Platform™ Software

ForgeRock Identity Platform™ serves as the basis for our simple and comprehensive Identity and Access Management solution. We help our customers deepen their relationships with their customers, and improve the productivity and connectivity of their employees and partners. For more information about ForgeRock and about the platform, see https://www.forgerock.com.

Chapter 1

Amster Entity Reference

This chapter contains details of the entities available to Amster in AM 7.

AcceptTermsAndConditions

Realm Operations

Resource path: `/realm-config/authentication/authenticationtrees/nodes/AcceptTermsAndConditionsNode`

Resource version: `1.0`

create

Usage:

```
am> create AcceptTermsAndConditions --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "required" : [ ]
}
```

delete

Usage:

```
am> delete AcceptTermsAndConditions --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action AcceptTermsAndConditions --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action AcceptTermsAndConditions --realm Realm --actionName getCreatableTypes
```

listOutcomes

List the available outcomes for the node type.

Usage:

```
am> action AcceptTermsAndConditions --realm Realm --body body --actionName listOutcomes
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "title" : "Some configuration of the node. This does not need to be complete against the
 configuration schema."
}
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action AcceptTermsAndConditions --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query AcceptTermsAndConditions --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read AcceptTermsAndConditions --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update AcceptTermsAndConditions --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "required" : [ ]
}
```

AccountActiveCheck

Realm Operations

Resource path: `/realm-config/authentication/modules/accountactivecheck`

Resource version: `1.0`

create

Usage:

```
am> create AccountActiveCheck --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "authenticationLevel" : {
      "title" : "Authentication Level",
      "description" : "The authentication level associated with this module.<br><br>Each
 authentication module has an authentication level that can be used to indicate the level of security
 associated with the module; 0 is the lowest (and the default).",
      "propertyOrder" : null,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    }
  }
}
```

delete

Usage:

```
am> delete AccountActiveCheck --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action AccountActiveCheck --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action AccountActiveCheck --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action AccountActiveCheck --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query AccountActiveCheck --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read AccountActiveCheck --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update AccountActiveCheck --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "authenticationLevel" : {
      "title" : "Authentication Level",
      "description" : "The authentication level associated with this module.<br><br>Each
 authentication module has an authentication level that can be used to indicate the level of security
 associated with the module; 0 is the lowest (and the default).",
      "propertyOrder" : null,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    }
  }
}
```

Global Operations

Resource path: `/global-config/authentication/modules/accountactivecheck`

Resource version: `1.0`

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action AccountActiveCheck --global --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action AccountActiveCheck --global --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action AccountActiveCheck --global --actionName nextdescendents
```

read

Usage:

```
am> read AccountActiveCheck --global
```

update

Usage:

```
am> update AccountActiveCheck --global --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "defaults" : {
      "properties" : {
        "authenticationLevel" : {
          "title" : "Authentication Level",
          "description" : "The authentication level associated with this module.<br><br>Each
 authentication module has an authentication level that can be used to indicate the level of security
 associated with the module; 0 is the lowest (and the default).",
          "propertyOrder" : null,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        }
      },
      "type" : "object",
      "title" : "Realm Defaults"
    }
  }
}
```

AccountActiveDecision

Realm Operations

Resource path: `/realm-config/authentication/authenticationtrees/nodes/AccountActiveDecisionNode`

Resource version: `1.0`

create

Usage:

```
am> create AccountActiveDecision --realm Realm --id id --body body
```

Parameters:

`--id`

The unique identifier for the resource.

`--body`

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "required" : [ ]
}
```

delete

Usage:

```
am> delete AccountActiveDecision --realm Realm --id id
```

Parameters:

`--id`

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action AccountActiveDecision --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action AccountActiveDecision --realm Realm --actionName getCreatableTypes
```

listOutcomes

List the available outcomes for the node type.

Usage:

```
am> action AccountActiveDecision --realm Realm --body body --actionName listOutcomes
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "title" : "Some configuration of the node. This does not need to be complete against the
 configuration schema."
}
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action AccountActiveDecision --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query AccountActiveDecision --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read AccountActiveDecision --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update AccountActiveDecision --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "required" : [ ]
}
```

AccountLockout

Realm Operations

Resource path: `/realm-config/authentication/authenticationtrees/nodes/AccountLockoutNode`

Resource version: `1.0`

create

Usage:

```
am> create AccountLockout --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "lockAction" : {
      "title" : "Lock Action",
      "description" : "If the action is set to LOCK, the node will lock the account.",
      "propertyOrder" : 100,
      "type" : "string",
      "exampleValue" : ""
    }
  },
  "required" : [ "lockAction" ]
}
```

delete

Usage:

```
am> delete AccountLockout --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action AccountLockout --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action AccountLockout --realm Realm --actionName getCreatableTypes
```

listOutcomes

List the available outcomes for the node type.

Usage:

```
am> action AccountLockout --realm Realm --body body --actionName listOutcomes
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "title" : "Some configuration of the node. This does not need to be complete against the
 configuration schema."
}
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action AccountLockout --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query AccountLockout --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read AccountLockout --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update AccountLockout --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "lockAction" : {
      "title" : "Lock Action",
      "description" : "If the action is set to LOCK, the node will lock the account.",
      "propertyOrder" : 100,
      "type" : "string",
      "exampleValue" : ""
    }
  },
  "required" : [ "lockAction" ]
}
```

ActiveDirectory

Realm Operations

Resource path: `/realm-config/services/id-repositories/LDAPv3ForAD`

Resource version: `1.0`

create

Usage:

```
am> create ActiveDirectory --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "pluginconfig" : {
      "type" : "object",
      "title" : "Plug-in Configuration",
      "propertyOrder" : 2,
      "properties" : {
        "sunIdRepoClass" : {
          "title" : "LDAPv3 Repository Plug-in Class Name",
          "description" : "",
          "propertyOrder" : 1700,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "sunIdRepoSupportedOperations" : {
          "title" : "LDAPv3 Plug-in Supported Types and Operations",
          "description" : "",
          "propertyOrder" : 1900,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "sunIdRepoAttributeMapping" : {
          "title" : "Attribute Name Mapping",
          "description" : "",
          "propertyOrder" : 1800,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        }
      }
    },
    "userconfig" : {
      "type" : "object",
      "title" : "User Configuration",
      "propertyOrder" : 3,
      "properties" : {
        "sun-idrepo-ldapv3-config-auth-kba-attempts-attr" : {
          "title" : "Knowledge Based Authentication Attempts Attribute Name",
          "description" : "",
          "propertyOrder" : 5410,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
```

```
        },
        "sun-idrepo-ldapv3-config-inactive" : {
          "title" : "User Status Inactive Value",
          "description" : "",
          "propertyOrder" : 2800,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-user-attributes" : {
          "title" : "LDAP User Attributes",
          "description" : "",
          "propertyOrder" : 2400,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-createuser-attr-mapping" : {
          "title" : "Create User Attribute Mapping",
          "description" : "Format: attribute name or TargetAttributeName=SourceAttributeName",
          "propertyOrder" : 2500,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-auth-kba-index-attr" : {
          "title" : "Knowledge Based Authentication Active Index",
          "description" : "",
          "propertyOrder" : 5400,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-people-container-value" : {
          "title" : "LDAP People Container Value",
          "description" : "",
          "propertyOrder" : 5100,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-people-container-name" : {
          "title" : "LDAP People Container Naming Attribute",
          "description" : "",
          "propertyOrder" : 5000,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-users-search-filter" : {
          "title" : "LDAP Users  Search Filter",
          "description" : "",
          "propertyOrder" : 2200,
```

```
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-user-objectclass" : {
          "title" : "LDAP User Object Class",
          "description" : "",
          "propertyOrder" : 2300,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-isactive" : {
          "title" : "Attribute Name of User Status",
          "description" : "",
          "propertyOrder" : 2600,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-active" : {
          "title" : "User Status Active Value",
          "description" : "",
          "propertyOrder" : 2700,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-auth-kba-attr" : {
          "title" : "Knowledge Based Authentication Attribute Name",
          "description" : "",
          "propertyOrder" : 5300,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-users-search-attribute" : {
          "title" : "LDAP Users  Search Attribute",
          "description" : "",
          "propertyOrder" : 2100,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "ldapsettings" : {
      "type" : "object",
      "title" : "Server Settings",
      "propertyOrder" : 0,
      "properties" : {
        "sun-idrepo-ldapv3-config-authpw" : {
          "title" : "LDAP Bind Password",
```

```
          "description" : "",
          "propertyOrder" : 800,
          "required" : false,
          "type" : "string",
          "format" : "password",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-connection_pool_max_size" : {
          "title" : "LDAP Connection Pool Maximum Size",
          "description" : "",
          "propertyOrder" : 1200,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-connection-mode" : {
          "title" : "LDAP Connection Mode",
          "description" : "Defines which protocol/operation is used to establish the connection to
the LDAP Directory Server.<br><br>If 'LDAP' is selected, the connection <b>won't be secured</b> and
passwords are transferred in <b>cleartext</b> over the network.<br/> If 'LDAPS' is selected, the
connection is secured via SSL or TLS. <br/> If 'StartTLS' is selected, the connection is secured by
using StartTLS extended operation.",
          "propertyOrder" : 1000,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-authid" : {
          "title" : "LDAP Bind DN",
          "description" : "A user or admin with sufficient access rights to perform the supported
operations.",
          "propertyOrder" : 700,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-time-limit" : {
          "title" : "Search Timeout",
          "description" : "In seconds.",
          "propertyOrder" : 1600,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-connection_pool_min_size" : {
          "title" : "LDAP Connection Pool Minimum Size",
          "description" : "",
          "propertyOrder" : 1100,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-max-result" : {
          "title" : "Maximum Results Returned from Search",
          "description" : "",
          "propertyOrder" : 1500,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
```

```
      },
      "openam-idrepo-ldapv3-heartbeat-interval" : {
        "title" : "LDAP Connection Heartbeat Interval",
        "description" : "Specifies how often should OpenAM send a heartbeat request to the
directory.<br><br>This setting controls how often OpenAM <b>should</b> send a heartbeat search
request to the configured directory. If a connection becomes unresponsive (e.g. due to a network
error) then it may take up to the interval period before the problem is detected. Use along with the
Heartbeat Time Unit parameter to define the exact interval. Zero or negative value will result in
disabling heartbeat requests.",
        "propertyOrder" : 1300,
        "required" : false,
        "type" : "integer",
        "exampleValue" : ""
      },
      "openam-idrepo-ldapv3-affinity-enabled" : {
        "title" : "Affinity Enabled",
        "description" : "Enables affinity based request load balancing when accessing the user store
servers (based on DN). It is imperative that the connection string setting is set to the same value
for all OpenAM servers in the deployment when this feature is enabled.",
        "propertyOrder" : 6200,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
      },
      "sun-idrepo-ldapv3-config-ldap-server" : {
        "title" : "LDAP Server",
        "description" : "Format: LDAP server host name:port | server_ID | site_ID",
        "propertyOrder" : 600,
        "required" : true,
        "items" : {
          "type" : "string"
        },
        "minItems" : 1,
        "type" : "array",
        "exampleValue" : ""
      },
      "sun-idrepo-ldapv3-config-search-scope" : {
        "title" : "LDAPv3 Plug-in Search Scope",
        "description" : "",
        "propertyOrder" : 2000,
        "required" : false,
        "type" : "string",
        "exampleValue" : ""
      },
      "sun-idrepo-ldapv3-config-organization_name" : {
        "title" : "LDAP Organization DN",
        "description" : "",
        "propertyOrder" : 900,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
      },
      "openam-idrepo-ldapv3-heartbeat-timeunit" : {
        "title" : "LDAP Connection Heartbeat Time Unit",
        "description" : "Defines the time unit corresponding to the Heartbeat Interval
setting.<br><br>This setting controls how often OpenAM <b>should</b> send a heartbeat search request
to the configured directory. If a connection becomes unresponsive (e.g. due to a network error) then
it may take up to the interval period before the problem is detected. Use along with the Heartbeat
Interval parameter to define the exact interval.",
```

```
        "propertyOrder" : 1400,
        "required" : false,
        "type" : "string",
        "exampleValue" : ""
      }
    }
  },
  "persistentsearch" : {
    "type" : "object",
    "title" : "Persistent Search Controls",
    "propertyOrder" : 7,
    "properties" : {
      "sun-idrepo-ldapv3-config-psearch-scope" : {
        "title" : "Persistent Search Scope",
        "description" : "",
        "propertyOrder" : 5700,
        "required" : false,
        "type" : "string",
        "exampleValue" : ""
      },
      "sun-idrepo-ldapv3-config-psearchbase" : {
        "title" : "Persistent Search Base DN",
        "description" : "",
        "propertyOrder" : 5500,
        "required" : false,
        "type" : "string",
        "exampleValue" : ""
      }
    }
  },
  "groupconfig" : {
    "type" : "object",
    "title" : "Group Configuration",
    "propertyOrder" : 5,
    "properties" : {
      "sun-idrepo-ldapv3-config-group-container-name" : {
        "title" : "LDAP Groups Container Naming Attribute",
        "description" : "",
        "propertyOrder" : 3100,
        "required" : false,
        "type" : "string",
        "exampleValue" : ""
      },
      "sun-idrepo-ldapv3-config-groups-search-filter" : {
        "title" : "LDAP Groups Search Filter",
        "description" : "",
        "propertyOrder" : 3000,
        "required" : false,
        "type" : "string",
        "exampleValue" : ""
      },
      "sun-idrepo-ldapv3-config-memberof" : {
        "title" : "Attribute Name for Group Membership",
        "description" : "",
        "propertyOrder" : 3500,
        "required" : false,
        "type" : "string",
        "exampleValue" : ""
      },
```

```
       "sun-idrepo-ldapv3-config-group-objectclass" : {
         "title" : "LDAP Groups Object Class",
         "description" : "",
         "propertyOrder" : 3300,
         "required" : false,
         "items" : {
           "type" : "string"
         },
         "type" : "array",
         "exampleValue" : ""
       },
       "sun-idrepo-ldapv3-config-uniquemember" : {
         "title" : "Attribute Name of Unique Member",
         "description" : "",
         "propertyOrder" : 3600,
         "required" : false,
         "type" : "string",
         "exampleValue" : ""
       },
       "adRecursiveGroupMembership" : {
         "title" : "AD Recursive Group Membership Evaluation",
         "description" : "Used to enable/disable Active Directory Recursive Group
Membership evaluation.<br><br>Enables an Active Directory specific extensible filter called
LDAP_MATCHING_RULE_IN_CHAIN that according to MSDN \"walks the chain of ancestry in objects all
the way to the root until it finds a match\", meaning that it will resolve all group memberships,
including nested groups. This will add a performance overhead on the Active Directory server, indexes
may need to be created.",
         "propertyOrder" : 6100,
         "required" : true,
         "type" : "boolean",
         "exampleValue" : ""
       },
       "sun-idrepo-ldapv3-config-groups-search-attribute" : {
         "title" : "LDAP Groups Search Attribute",
         "description" : "",
         "propertyOrder" : 2900,
         "required" : false,
         "type" : "string",
         "exampleValue" : ""
       },
       "sun-idrepo-ldapv3-config-group-container-value" : {
         "title" : "LDAP Groups Container Value",
         "description" : "",
         "propertyOrder" : 3200,
         "required" : false,
         "type" : "string",
         "exampleValue" : ""
       },
       "sun-idrepo-ldapv3-config-group-attributes" : {
         "title" : "LDAP Groups Attributes",
         "description" : "",
         "propertyOrder" : 3400,
         "required" : false,
         "items" : {
           "type" : "string"
         },
         "type" : "array",
         "exampleValue" : ""
       }
```

```
      }
    },
    "authentication" : {
      "type" : "object",
      "title" : "Authentication Configuration",
      "propertyOrder" : 4,
      "properties" : {
        "sun-idrepo-ldapv3-config-auth-naming-attr" : {
          "title" : "Authentication Naming Attribute",
          "description" : "",
          "propertyOrder" : 5200,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "errorhandling" : {
      "type" : "object",
      "title" : "Error Handling Configuration",
      "propertyOrder" : 8,
      "properties" : {
        "com.iplanet.am.ldap.connection.delay.between.retries" : {
          "title" : "The Delay Time Between Retries",
          "description" : "In milliseconds.",
          "propertyOrder" : 5800,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        }
      }
    },
    "cachecontrol" : {
      "type" : "object",
      "title" : "Cache Control",
      "propertyOrder" : 9,
      "properties" : {
        "sun-idrepo-ldapv3-dncache-size" : {
          "title" : "DN Cache Size",
          "description" : "In DN items, only used when DN Cache is enabled.",
          "propertyOrder" : 6000,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-dncache-enabled" : {
          "title" : "DN Cache",
          "description" : "Used to enable/disable the DN Cache within the OpenAM repository
implementation.<br><br>The DN Cache is used to cache DN lookups which tend to happen in bursts during
authentication. The DN Cache can become out of date when a user is moved or renamed in the underlying
LDAP store and this is not reflected in a persistent search result. Enable when the underlying LDAP
store supports persistent search and move/rename (mod_dn) results are available.",
          "propertyOrder" : 5900,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        }
      }
    }
```

```
  }
}
```

delete

Usage:

```
am> delete ActiveDirectory --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action ActiveDirectory --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action ActiveDirectory --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action ActiveDirectory --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query ActiveDirectory --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read ActiveDirectory --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update ActiveDirectory --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "pluginconfig" : {
      "type" : "object",
      "title" : "Plug-in Configuration",
      "propertyOrder" : 2,
      "properties" : {
        "sunIdRepoClass" : {
          "title" : "LDAPv3 Repository Plug-in Class Name",
          "description" : "",
          "propertyOrder" : 1700,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "sunIdRepoSupportedOperations" : {
          "title" : "LDAPv3 Plug-in Supported Types and Operations",
          "description" : "",
          "propertyOrder" : 1900,
          "required" : false,
          "items" : {
```

```
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "sunIdRepoAttributeMapping" : {
          "title" : "Attribute Name Mapping",
          "description" : "",
          "propertyOrder" : 1800,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        }
      }
    },
    "userconfig" : {
      "type" : "object",
      "title" : "User Configuration",
      "propertyOrder" : 3,
      "properties" : {
        "sun-idrepo-ldapv3-config-auth-kba-attempts-attr" : {
          "title" : "Knowledge Based Authentication Attempts Attribute Name",
          "description" : "",
          "propertyOrder" : 5410,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-inactive" : {
          "title" : "User Status Inactive Value",
          "description" : "",
          "propertyOrder" : 2800,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-user-attributes" : {
          "title" : "LDAP User Attributes",
          "description" : "",
          "propertyOrder" : 2400,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-createuser-attr-mapping" : {
          "title" : "Create User Attribute Mapping",
          "description" : "Format: attribute name or TargetAttributeName=SourceAttributeName",
          "propertyOrder" : 2500,
          "required" : false,
          "items" : {
```

```
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-auth-kba-index-attr" : {
          "title" : "Knowledge Based Authentication Active Index",
          "description" : "",
          "propertyOrder" : 5400,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-people-container-value" : {
          "title" : "LDAP People Container Value",
          "description" : "",
          "propertyOrder" : 5100,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-people-container-name" : {
          "title" : "LDAP People Container Naming Attribute",
          "description" : "",
          "propertyOrder" : 5000,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-users-search-filter" : {
          "title" : "LDAP Users  Search Filter",
          "description" : "",
          "propertyOrder" : 2200,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-user-objectclass" : {
          "title" : "LDAP User Object Class",
          "description" : "",
          "propertyOrder" : 2300,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-isactive" : {
          "title" : "Attribute Name of User Status",
          "description" : "",
          "propertyOrder" : 2600,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-active" : {
          "title" : "User Status Active Value",
          "description" : "",
```

```
          "propertyOrder" : 2700,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-auth-kba-attr" : {
          "title" : "Knowledge Based Authentication Attribute Name",
          "description" : "",
          "propertyOrder" : 5300,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-users-search-attribute" : {
          "title" : "LDAP Users  Search Attribute",
          "description" : "",
          "propertyOrder" : 2100,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "ldapsettings" : {
      "type" : "object",
      "title" : "Server Settings",
      "propertyOrder" : 0,
      "properties" : {
        "sun-idrepo-ldapv3-config-authpw" : {
          "title" : "LDAP Bind Password",
          "description" : "",
          "propertyOrder" : 800,
          "required" : false,
          "type" : "string",
          "format" : "password",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-connection_pool_max_size" : {
          "title" : "LDAP Connection Pool Maximum Size",
          "description" : "",
          "propertyOrder" : 1200,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-connection-mode" : {
          "title" : "LDAP Connection Mode",
          "description" : "Defines which protocol/operation is used to establish the connection to
the LDAP Directory Server.<br><br>If 'LDAP' is selected, the connection <b>won't be secured</b> and
passwords are transferred in <b>cleartext</b> over the network.<br/> If 'LDAPS' is selected, the
connection is secured via SSL or TLS. <br/> If 'StartTLS' is selected, the connection is secured by
using StartTLS extended operation.",
          "propertyOrder" : 1000,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
```

```
      },
      "sun-idrepo-ldapv3-config-authid" : {
        "title" : "LDAP Bind DN",
        "description" : "A user or admin with sufficient access rights to perform the supported
operations.",
        "propertyOrder" : 700,
        "required" : false,
        "type" : "string",
        "exampleValue" : ""
      },
      "sun-idrepo-ldapv3-config-time-limit" : {
        "title" : "Search Timeout",
        "description" : "In seconds.",
        "propertyOrder" : 1600,
        "required" : false,
        "type" : "integer",
        "exampleValue" : ""
      },
      "sun-idrepo-ldapv3-config-connection_pool_min_size" : {
        "title" : "LDAP Connection Pool Minimum Size",
        "description" : "",
        "propertyOrder" : 1100,
        "required" : false,
        "type" : "integer",
        "exampleValue" : ""
      },
      "sun-idrepo-ldapv3-config-max-result" : {
        "title" : "Maximum Results Returned from Search",
        "description" : "",
        "propertyOrder" : 1500,
        "required" : false,
        "type" : "integer",
        "exampleValue" : ""
      },
      "openam-idrepo-ldapv3-heartbeat-interval" : {
        "title" : "LDAP Connection Heartbeat Interval",
        "description" : "Specifies how often should OpenAM send a heartbeat request to the
directory.<br><br>This setting controls how often OpenAM <b>should</b> send a heartbeat search
request to the configured directory. If a connection becomes unresponsive (e.g. due to a network
error) then it may take up to the interval period before the problem is detected. Use along with the
Heartbeat Time Unit parameter to define the exact interval. Zero or negative value will result in
disabling heartbeat requests.",
        "propertyOrder" : 1300,
        "required" : false,
        "type" : "integer",
        "exampleValue" : ""
      },
      "openam-idrepo-ldapv3-affinity-enabled" : {
        "title" : "Affinity Enabled",
        "description" : "Enables affinity based request load balancing when accessing the user store
servers (based on DN). It is imperative that the connection string setting is set to the same value
for all OpenAM servers in the deployment when this feature is enabled.",
        "propertyOrder" : 6200,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
      },
      "sun-idrepo-ldapv3-config-ldap-server" : {
        "title" : "LDAP Server",
```

```
          "description" : "Format: LDAP server host name:port | server_ID | site_ID",
          "propertyOrder" : 600,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "minItems" : 1,
          "type" : "array",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-search-scope" : {
          "title" : "LDAPv3 Plug-in Search Scope",
          "description" : "",
          "propertyOrder" : 2000,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-organization_name" : {
          "title" : "LDAP Organization DN",
          "description" : "",
          "propertyOrder" : 900,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "openam-idrepo-ldapv3-heartbeat-timeunit" : {
          "title" : "LDAP Connection Heartbeat Time Unit",
          "description" : "Defines the time unit corresponding to the Heartbeat Interval
setting.<br><br>This setting controls how often OpenAM <b>should</b> send a heartbeat search request
to the configured directory. If a connection becomes unresponsive (e.g. due to a network error) then
it may take up to the interval period before the problem is detected. Use along with the Heartbeat
Interval parameter to define the exact interval.",
          "propertyOrder" : 1400,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "persistentsearch" : {
      "type" : "object",
      "title" : "Persistent Search Controls",
      "propertyOrder" : 7,
      "properties" : {
        "sun-idrepo-ldapv3-config-psearch-scope" : {
          "title" : "Persistent Search Scope",
          "description" : "",
          "propertyOrder" : 5700,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-psearchbase" : {
          "title" : "Persistent Search Base DN",
          "description" : "",
          "propertyOrder" : 5500,
          "required" : false,
          "type" : "string",
```

```
          "exampleValue" : ""
        }
      }
    },
    "groupconfig" : {
      "type" : "object",
      "title" : "Group Configuration",
      "propertyOrder" : 5,
      "properties" : {
        "sun-idrepo-ldapv3-config-group-container-name" : {
          "title" : "LDAP Groups Container Naming Attribute",
          "description" : "",
          "propertyOrder" : 3100,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-groups-search-filter" : {
          "title" : "LDAP Groups Search Filter",
          "description" : "",
          "propertyOrder" : 3000,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-memberof" : {
          "title" : "Attribute Name for Group Membership",
          "description" : "",
          "propertyOrder" : 3500,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-group-objectclass" : {
          "title" : "LDAP Groups Object Class",
          "description" : "",
          "propertyOrder" : 3300,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-uniquemember" : {
          "title" : "Attribute Name of Unique Member",
          "description" : "",
          "propertyOrder" : 3600,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "adRecursiveGroupMembership" : {
          "title" : "AD Recursive Group Membership Evaluation",
          "description" : "Used to enable/disable Active Directory Recursive Group
Membership evaluation.<br><br>Enables an Active Directory specific extensible filter called
LDAP_MATCHING_RULE_IN_CHAIN that according to MSDN \"walks the chain of ancestry in objects all
the way to the root until it finds a match\", meaning that it will resolve all group memberships,
```

```
including nested groups. This will add a performance overhead on the Active Directory server, indexes
may need to be created.",
          "propertyOrder" : 6100,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-groups-search-attribute" : {
          "title" : "LDAP Groups Search Attribute",
          "description" : "",
          "propertyOrder" : 2900,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-group-container-value" : {
          "title" : "LDAP Groups Container Value",
          "description" : "",
          "propertyOrder" : 3200,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-group-attributes" : {
          "title" : "LDAP Groups Attributes",
          "description" : "",
          "propertyOrder" : 3400,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        }
      }
    },
    "authentication" : {
      "type" : "object",
      "title" : "Authentication Configuration",
      "propertyOrder" : 4,
      "properties" : {
        "sun-idrepo-ldapv3-config-auth-naming-attr" : {
          "title" : "Authentication Naming Attribute",
          "description" : "",
          "propertyOrder" : 5200,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "errorhandling" : {
      "type" : "object",
      "title" : "Error Handling Configuration",
      "propertyOrder" : 8,
      "properties" : {
        "com.iplanet.am.ldap.connection.delay.between.retries" : {
          "title" : "The Delay Time Between Retries",
          "description" : "In milliseconds.",
```

```
          "propertyOrder" : 5800,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        }
      }
    },
    "cachecontrol" : {
      "type" : "object",
      "title" : "Cache Control",
      "propertyOrder" : 9,
      "properties" : {
        "sun-idrepo-ldapv3-dncache-size" : {
          "title" : "DN Cache Size",
          "description" : "In DN items, only used when DN Cache is enabled.",
          "propertyOrder" : 6000,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-dncache-enabled" : {
          "title" : "DN Cache",
          "description" : "Used to enable/disable the DN Cache within the OpenAM repository
 implementation.<br><br>The DN Cache is used to cache DN lookups which tend to happen in bursts during
 authentication. The DN Cache can become out of date when a user is moved or renamed in the underlying
 LDAP store and this is not reflected in a persistent search result. Enable when the underlying LDAP
 store supports persistent search and move/rename (mod_dn) results are available.",
          "propertyOrder" : 5900,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        }
      }
    }
  }
}
```

ActiveDirectoryApplicationModeADAM

Realm Operations

Resource path: `/realm-config/services/id-repositories/LDAPv3ForADAM`

Resource version: `1.0`

create

Usage:

```
am> create ActiveDirectoryApplicationModeADAM --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "cachecontrol" : {
      "type" : "object",
      "title" : "Cache Control",
      "propertyOrder" : 9,
      "properties" : {
        "sun-idrepo-ldapv3-dncache-size" : {
          "title" : "DN Cache Size",
          "description" : "In DN items, only used when DN Cache is enabled.",
          "propertyOrder" : 6000,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-dncache-enabled" : {
          "title" : "DN Cache",
          "description" : "Used to enable/disable the DN Cache within the OpenAM repository
 implementation.<br><br>The DN Cache is used to cache DN lookups which tend to happen in bursts during
 authentication. The DN Cache can become out of date when a user is moved or renamed in the underlying
 LDAP store and this is not reflected in a persistent search result. Enable when the underlying LDAP
 store supports persistent search and move/rename (mod_dn) results are available.",
          "propertyOrder" : 5900,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        }
      }
    },
    "ldapsettings" : {
      "type" : "object",
      "title" : "Server Settings",
      "propertyOrder" : 0,
      "properties" : {
        "sun-idrepo-ldapv3-config-max-result" : {
          "title" : "Maximum Results Returned from Search",
          "description" : "",
          "propertyOrder" : 1500,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "openam-idrepo-ldapv3-heartbeat-interval" : {
          "title" : "LDAP Connection Heartbeat Interval",
          "description" : "Specifies how often should OpenAM send a heartbeat request to the
 directory.<br><br>This setting controls how often OpenAM <b>should</b> send a heartbeat search
 request to the configured directory. If a connection becomes unresponsive (e.g. due to a network
 error) then it may take up to the interval period before the problem is detected. Use along with the
```

```
Heartbeat Time Unit parameter to define the exact interval. Zero or negative value will result in
disabling heartbeat requests.",
         "propertyOrder" : 1300,
         "required" : false,
         "type" : "integer",
         "exampleValue" : ""
       },
       "sun-idrepo-ldapv3-config-search-scope" : {
         "title" : "LDAPv3 Plug-in Search Scope",
         "description" : "",
         "propertyOrder" : 2000,
         "required" : false,
         "type" : "string",
         "exampleValue" : ""
       },
       "sun-idrepo-ldapv3-config-time-limit" : {
         "title" : "Search Timeout",
         "description" : "In seconds.",
         "propertyOrder" : 1600,
         "required" : false,
         "type" : "integer",
         "exampleValue" : ""
       },
       "sun-idrepo-ldapv3-config-connection_pool_max_size" : {
         "title" : "LDAP Connection Pool Maximum Size",
         "description" : "",
         "propertyOrder" : 1200,
         "required" : false,
         "type" : "integer",
         "exampleValue" : ""
       },
       "openam-idrepo-ldapv3-heartbeat-timeunit" : {
         "title" : "LDAP Connection Heartbeat Time Unit",
         "description" : "Defines the time unit corresponding to the Heartbeat Interval
setting.<br><br>This setting controls how often OpenAM <b>should</b> send a heartbeat search request
to the configured directory. If a connection becomes unresponsive (e.g. due to a network error) then
it may take up to the interval period before the problem is detected. Use along with the Heartbeat
Interval parameter to define the exact interval.",
         "propertyOrder" : 1400,
         "required" : false,
         "type" : "string",
         "exampleValue" : ""
       },
       "openam-idrepo-ldapv3-affinity-enabled" : {
         "title" : "Affinity Enabled",
         "description" : "Enables affinity based request load balancing when accessing the user store
servers (based on DN). It is imperative that the connection string setting is set to the same value
for all OpenAM servers in the deployment when this feature is enabled.",
         "propertyOrder" : 6200,
         "required" : true,
         "type" : "boolean",
         "exampleValue" : ""
       },
       "sun-idrepo-ldapv3-config-organization_name" : {
         "title" : "LDAP Organization DN",
         "description" : "",
         "propertyOrder" : 900,
         "required" : true,
         "type" : "string",
```

```
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-ldap-server" : {
          "title" : "LDAP Server",
          "description" : "Format: LDAP server host name:port | server_ID | site_ID",
          "propertyOrder" : 600,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "minItems" : 1,
          "type" : "array",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-connection_pool_min_size" : {
          "title" : "LDAP Connection Pool Minimum Size",
          "description" : "",
          "propertyOrder" : 1100,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-connection-mode" : {
          "title" : "LDAP Connection Mode",
          "description" : "Defines which protocol/operation is used to establish the connection to
the LDAP Directory Server.<br><br>If 'LDAP' is selected, the connection <b>won't be secured</b> and
passwords are transferred in <b>cleartext</b> over the network.<br/> If 'LDAPS' is selected, the
connection is secured via SSL or TLS. <br/> If 'StartTLS' is selected, the connection is secured by
using StartTLS extended operation.",
          "propertyOrder" : 1000,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-authid" : {
          "title" : "LDAP Bind DN",
          "description" : "A user or admin with sufficient access rights to perform the supported
operations.",
          "propertyOrder" : 700,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-authpw" : {
          "title" : "LDAP Bind Password",
          "description" : "",
          "propertyOrder" : 800,
          "required" : false,
          "type" : "string",
          "format" : "password",
          "exampleValue" : ""
        }
      }
    },
    "groupconfig" : {
      "type" : "object",
      "title" : "Group Configuration",
      "propertyOrder" : 5,
      "properties" : {
```

```
        "sun-idrepo-ldapv3-config-group-objectclass" : {
          "title" : "LDAP Groups Object Class",
          "description" : "",
          "propertyOrder" : 3300,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-groups-search-attribute" : {
          "title" : "LDAP Groups Search Attribute",
          "description" : "",
          "propertyOrder" : 2900,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-memberof" : {
          "title" : "Attribute Name for Group Membership",
          "description" : "",
          "propertyOrder" : 3500,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-group-container-value" : {
          "title" : "LDAP Groups Container Value",
          "description" : "",
          "propertyOrder" : 3200,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-group-container-name" : {
          "title" : "LDAP Groups Container Naming Attribute",
          "description" : "",
          "propertyOrder" : 3100,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-groups-search-filter" : {
          "title" : "LDAP Groups Search Filter",
          "description" : "",
          "propertyOrder" : 3000,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-uniquemember" : {
          "title" : "Attribute Name of Unique Member",
          "description" : "",
          "propertyOrder" : 3600,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
```

```
       "adRecursiveGroupMembership" : {
         "title" : "AD Recursive Group Membership Evaluation",
         "description" : "Used to enable/disable Active Directory Recursive Group
Membership evaluation.<br><br>Enables an Active Directory specific extensible filter called
LDAP_MATCHING_RULE_IN_CHAIN that according to MSDN \"walks the chain of ancestry in objects all
the way to the root until it finds a match\", meaning that it will resolve all group memberships,
including nested groups. This will add a performance overhead on the Active Directory server, indexes
may need to be created.",
         "propertyOrder" : 6100,
         "required" : true,
         "type" : "boolean",
         "exampleValue" : ""
       },
       "sun-idrepo-ldapv3-config-group-attributes" : {
         "title" : "LDAP Groups Attributes",
         "description" : "",
         "propertyOrder" : 3400,
         "required" : false,
         "items" : {
           "type" : "string"
         },
         "type" : "array",
         "exampleValue" : ""
       }
     }
   },
   "userconfig" : {
     "type" : "object",
     "title" : "User Configuration",
     "propertyOrder" : 3,
     "properties" : {
       "sun-idrepo-ldapv3-config-auth-kba-index-attr" : {
         "title" : "Knowledge Based Authentication Active Index",
         "description" : "",
         "propertyOrder" : 5400,
         "required" : false,
         "type" : "string",
         "exampleValue" : ""
       },
       "sun-idrepo-ldapv3-config-auth-kba-attr" : {
         "title" : "Knowledge Based Authentication Attribute Name",
         "description" : "",
         "propertyOrder" : 5300,
         "required" : false,
         "items" : {
           "type" : "string"
         },
         "type" : "array",
         "exampleValue" : ""
       },
       "sun-idrepo-ldapv3-config-isactive" : {
         "title" : "Attribute Name of User Status",
         "description" : "",
         "propertyOrder" : 2600,
         "required" : false,
         "type" : "string",
         "exampleValue" : ""
       },
       "sun-idrepo-ldapv3-config-people-container-name" : {
```

```
          "title" : "LDAP People Container Naming Attribute",
          "description" : "",
          "propertyOrder" : 5000,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-users-search-filter" : {
          "title" : "LDAP Users  Search Filter",
          "description" : "",
          "propertyOrder" : 2200,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-inactive" : {
          "title" : "User Status Inactive Value",
          "description" : "",
          "propertyOrder" : 2800,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-user-objectclass" : {
          "title" : "LDAP User Object Class",
          "description" : "",
          "propertyOrder" : 2300,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-users-search-attribute" : {
          "title" : "LDAP Users  Search Attribute",
          "description" : "",
          "propertyOrder" : 2100,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-active" : {
          "title" : "User Status Active Value",
          "description" : "",
          "propertyOrder" : 2700,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-auth-kba-attempts-attr" : {
          "title" : "Knowledge Based Authentication Attempts Attribute Name",
          "description" : "",
          "propertyOrder" : 5410,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
```

```
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-user-attributes" : {
          "title" : "LDAP User Attributes",
          "description" : "",
          "propertyOrder" : 2400,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-people-container-value" : {
          "title" : "LDAP People Container Value",
          "description" : "",
          "propertyOrder" : 5100,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-createuser-attr-mapping" : {
          "title" : "Create User Attribute Mapping",
          "description" : "Format: attribute name or TargetAttributeName=SourceAttributeName",
          "propertyOrder" : 2500,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        }
      }
    },
    "pluginconfig" : {
      "type" : "object",
      "title" : "Plug-in Configuration",
      "propertyOrder" : 2,
      "properties" : {
        "sunIdRepoClass" : {
          "title" : "LDAPv3 Repository Plug-in Class Name",
          "description" : "",
          "propertyOrder" : 1700,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "sunIdRepoAttributeMapping" : {
          "title" : "Attribute Name Mapping",
          "description" : "",
          "propertyOrder" : 1800,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "sunIdRepoSupportedOperations" : {
```

```
          "title" : "LDAPv3 Plug-in Supported Types and Operations",
          "description" : "",
          "propertyOrder" : 1900,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        }
      }
    },
    "persistentsearch" : {
      "type" : "object",
      "title" : "Persistent Search Controls",
      "propertyOrder" : 7,
      "properties" : {
        "sun-idrepo-ldapv3-config-psearch-scope" : {
          "title" : "Persistent Search Scope",
          "description" : "",
          "propertyOrder" : 5700,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-psearchbase" : {
          "title" : "Persistent Search Base DN",
          "description" : "",
          "propertyOrder" : 5500,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "authentication" : {
      "type" : "object",
      "title" : "Authentication Configuration",
      "propertyOrder" : 4,
      "properties" : {
        "sun-idrepo-ldapv3-config-auth-naming-attr" : {
          "title" : "Authentication Naming Attribute",
          "description" : "",
          "propertyOrder" : 5200,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "errorhandling" : {
      "type" : "object",
      "title" : "Error Handling Configuration",
      "propertyOrder" : 8,
      "properties" : {
        "com.iplanet.am.ldap.connection.delay.between.retries" : {
          "title" : "The Delay Time Between Retries",
          "description" : "In milliseconds.",
          "propertyOrder" : 5800,
```

```
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        }
      }
    }
  }
}
```

delete

Usage:

```
am> delete ActiveDirectoryApplicationModeADAM --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action ActiveDirectoryApplicationModeADAM --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action ActiveDirectoryApplicationModeADAM --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action ActiveDirectoryApplicationModeADAM --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query ActiveDirectoryApplicationModeADAM --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read ActiveDirectoryApplicationModeADAM --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update ActiveDirectoryApplicationModeADAM --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "cachecontrol" : {
      "type" : "object",
      "title" : "Cache Control",
      "propertyOrder" : 9,
      "properties" : {
        "sun-idrepo-ldapv3-dncache-size" : {
          "title" : "DN Cache Size",
          "description" : "In DN items, only used when DN Cache is enabled.",
          "propertyOrder" : 6000,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-dncache-enabled" : {
```

```
          "title" : "DN Cache",
          "description" : "Used to enable/disable the DN Cache within the OpenAM repository
implementation.<br><br>The DN Cache is used to cache DN lookups which tend to happen in bursts during
authentication. The DN Cache can become out of date when a user is moved or renamed in the underlying
LDAP store and this is not reflected in a persistent search result. Enable when the underlying LDAP
store supports persistent search and move/rename (mod_dn) results are available.",
          "propertyOrder" : 5900,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        }
      }
    },
    "ldapsettings" : {
      "type" : "object",
      "title" : "Server Settings",
      "propertyOrder" : 0,
      "properties" : {
        "sun-idrepo-ldapv3-config-max-result" : {
          "title" : "Maximum Results Returned from Search",
          "description" : "",
          "propertyOrder" : 1500,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "openam-idrepo-ldapv3-heartbeat-interval" : {
          "title" : "LDAP Connection Heartbeat Interval",
          "description" : "Specifies how often should OpenAM send a heartbeat request to the
directory.<br><br>This setting controls how often OpenAM <b>should</b> send a heartbeat search
request to the configured directory. If a connection becomes unresponsive (e.g. due to a network
error) then it may take up to the interval period before the problem is detected. Use along with the
Heartbeat Time Unit parameter to define the exact interval. Zero or negative value will result in
disabling heartbeat requests.",
          "propertyOrder" : 1300,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-search-scope" : {
          "title" : "LDAPv3 Plug-in Search Scope",
          "description" : "",
          "propertyOrder" : 2000,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-time-limit" : {
          "title" : "Search Timeout",
          "description" : "In seconds.",
          "propertyOrder" : 1600,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-connection_pool_max_size" : {
          "title" : "LDAP Connection Pool Maximum Size",
          "description" : "",
          "propertyOrder" : 1200,
```

```
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "openam-idrepo-ldapv3-heartbeat-timeunit" : {
          "title" : "LDAP Connection Heartbeat Time Unit",
          "description" : "Defines the time unit corresponding to the Heartbeat Interval
setting.<br><br>This setting controls how often OpenAM <b>should</b> send a heartbeat search request
to the configured directory. If a connection becomes unresponsive (e.g. due to a network error) then
it may take up to the interval period before the problem is detected. Use along with the Heartbeat
Interval parameter to define the exact interval.",
          "propertyOrder" : 1400,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "openam-idrepo-ldapv3-affinity-enabled" : {
          "title" : "Affinity Enabled",
          "description" : "Enables affinity based request load balancing when accessing the user store
servers (based on DN). It is imperative that the connection string setting is set to the same value
for all OpenAM servers in the deployment when this feature is enabled.",
          "propertyOrder" : 6200,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-organization_name" : {
          "title" : "LDAP Organization DN",
          "description" : "",
          "propertyOrder" : 900,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-ldap-server" : {
          "title" : "LDAP Server",
          "description" : "Format: LDAP server host name:port | server_ID | site_ID",
          "propertyOrder" : 600,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "minItems" : 1,
          "type" : "array",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-connection_pool_min_size" : {
          "title" : "LDAP Connection Pool Minimum Size",
          "description" : "",
          "propertyOrder" : 1100,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-connection-mode" : {
          "title" : "LDAP Connection Mode",
          "description" : "Defines which protocol/operation is used to establish the connection to
the LDAP Directory Server.<br><br>If 'LDAP' is selected, the connection <b>won't be secured</b> and
passwords are transferred in <b>cleartext</b> over the network.<br/> If 'LDAPS' is selected, the
```

```
connection is secured via SSL or TLS. <br/> If 'StartTLS' is selected, the connection is secured by
using StartTLS extended operation.",
         "propertyOrder" : 1000,
         "required" : false,
         "type" : "string",
         "exampleValue" : ""
       },
       "sun-idrepo-ldapv3-config-authid" : {
         "title" : "LDAP Bind DN",
         "description" : "A user or admin with sufficient access rights to perform the supported
operations.",
         "propertyOrder" : 700,
         "required" : false,
         "type" : "string",
         "exampleValue" : ""
       },
       "sun-idrepo-ldapv3-config-authpw" : {
         "title" : "LDAP Bind Password",
         "description" : "",
         "propertyOrder" : 800,
         "required" : false,
         "type" : "string",
         "format" : "password",
         "exampleValue" : ""
       }
     }
   },
   "groupconfig" : {
     "type" : "object",
     "title" : "Group Configuration",
     "propertyOrder" : 5,
     "properties" : {
       "sun-idrepo-ldapv3-config-group-objectclass" : {
         "title" : "LDAP Groups Object Class",
         "description" : "",
         "propertyOrder" : 3300,
         "required" : false,
         "items" : {
           "type" : "string"
         },
         "type" : "array",
         "exampleValue" : ""
       },
       "sun-idrepo-ldapv3-config-groups-search-attribute" : {
         "title" : "LDAP Groups Search Attribute",
         "description" : "",
         "propertyOrder" : 2900,
         "required" : false,
         "type" : "string",
         "exampleValue" : ""
       },
       "sun-idrepo-ldapv3-config-memberof" : {
         "title" : "Attribute Name for Group Membership",
         "description" : "",
         "propertyOrder" : 3500,
         "required" : false,
         "type" : "string",
         "exampleValue" : ""
       },
```

```
        "sun-idrepo-ldapv3-config-group-container-value" : {
          "title" : "LDAP Groups Container Value",
          "description" : "",
          "propertyOrder" : 3200,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-group-container-name" : {
          "title" : "LDAP Groups Container Naming Attribute",
          "description" : "",
          "propertyOrder" : 3100,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-groups-search-filter" : {
          "title" : "LDAP Groups Search Filter",
          "description" : "",
          "propertyOrder" : 3000,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-uniquemember" : {
          "title" : "Attribute Name of Unique Member",
          "description" : "",
          "propertyOrder" : 3600,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "adRecursiveGroupMembership" : {
          "title" : "AD Recursive Group Membership Evaluation",
          "description" : "Used to enable/disable Active Directory Recursive Group
Membership evaluation.<br><br>Enables an Active Directory specific extensible filter called
LDAP_MATCHING_RULE_IN_CHAIN that according to MSDN \"walks the chain of ancestry in objects all
the way to the root until it finds a match\", meaning that it will resolve all group memberships,
including nested groups. This will add a performance overhead on the Active Directory server, indexes
may need to be created.",
          "propertyOrder" : 6100,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-group-attributes" : {
          "title" : "LDAP Groups Attributes",
          "description" : "",
          "propertyOrder" : 3400,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        }
      }
    },
    "userconfig" : {
```

```
      "type" : "object",
      "title" : "User Configuration",
      "propertyOrder" : 3,
      "properties" : {
        "sun-idrepo-ldapv3-config-auth-kba-index-attr" : {
          "title" : "Knowledge Based Authentication Active Index",
          "description" : "",
          "propertyOrder" : 5400,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-auth-kba-attr" : {
          "title" : "Knowledge Based Authentication Attribute Name",
          "description" : "",
          "propertyOrder" : 5300,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-isactive" : {
          "title" : "Attribute Name of User Status",
          "description" : "",
          "propertyOrder" : 2600,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-people-container-name" : {
          "title" : "LDAP People Container Naming Attribute",
          "description" : "",
          "propertyOrder" : 5000,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-users-search-filter" : {
          "title" : "LDAP Users  Search Filter",
          "description" : "",
          "propertyOrder" : 2200,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-inactive" : {
          "title" : "User Status Inactive Value",
          "description" : "",
          "propertyOrder" : 2800,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-user-objectclass" : {
          "title" : "LDAP User Object Class",
          "description" : "",
          "propertyOrder" : 2300,
```

```
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-users-search-attribute" : {
          "title" : "LDAP Users  Search Attribute",
          "description" : "",
          "propertyOrder" : 2100,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-active" : {
          "title" : "User Status Active Value",
          "description" : "",
          "propertyOrder" : 2700,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-auth-kba-attempts-attr" : {
          "title" : "Knowledge Based Authentication Attempts Attribute Name",
          "description" : "",
          "propertyOrder" : 5410,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-user-attributes" : {
          "title" : "LDAP User Attributes",
          "description" : "",
          "propertyOrder" : 2400,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-people-container-value" : {
          "title" : "LDAP People Container Value",
          "description" : "",
          "propertyOrder" : 5100,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-createuser-attr-mapping" : {
          "title" : "Create User Attribute Mapping",
          "description" : "Format: attribute name or TargetAttributeName=SourceAttributeName",
          "propertyOrder" : 2500,
          "required" : false,
          "items" : {
```

```
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        }
      }
    },
    "pluginconfig" : {
      "type" : "object",
      "title" : "Plug-in Configuration",
      "propertyOrder" : 2,
      "properties" : {
        "sunIdRepoClass" : {
          "title" : "LDAPv3 Repository Plug-in Class Name",
          "description" : "",
          "propertyOrder" : 1700,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "sunIdRepoAttributeMapping" : {
          "title" : "Attribute Name Mapping",
          "description" : "",
          "propertyOrder" : 1800,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "sunIdRepoSupportedOperations" : {
          "title" : "LDAPv3 Plug-in Supported Types and Operations",
          "description" : "",
          "propertyOrder" : 1900,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        }
      }
    },
    "persistentsearch" : {
      "type" : "object",
      "title" : "Persistent Search Controls",
      "propertyOrder" : 7,
      "properties" : {
        "sun-idrepo-ldapv3-config-psearch-scope" : {
          "title" : "Persistent Search Scope",
          "description" : "",
          "propertyOrder" : 5700,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-psearchbase" : {
          "title" : "Persistent Search Base DN",
```

```
          "description" : "",
          "propertyOrder" : 5500,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "authentication" : {
      "type" : "object",
      "title" : "Authentication Configuration",
      "propertyOrder" : 4,
      "properties" : {
        "sun-idrepo-ldapv3-config-auth-naming-attr" : {
          "title" : "Authentication Naming Attribute",
          "description" : "",
          "propertyOrder" : 5200,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "errorhandling" : {
      "type" : "object",
      "title" : "Error Handling Configuration",
      "propertyOrder" : 8,
      "properties" : {
        "com.iplanet.am.ldap.connection.delay.between.retries" : {
          "title" : "The Delay Time Between Retries",
          "description" : "In milliseconds.",
          "propertyOrder" : 5800,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        }
      }
    }
  }
}
```

ActiveDirectoryModule

Realm Operations

Resource path: `/realm-config/authentication/modules/activedirectory`

Resource version: `1.0`

create

Usage:

```
am> create ActiveDirectoryModule --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "trustAllServerCertificates" : {
      "title" : "Trust All Server Certificates",
      "description" : "Enables a <code>X509TrustManager</code> that trusts all
 certificates.<br><br>This feature will allow the LDAP authentication module to connect to LDAP
 servers protected by self signed or invalid certificates (such as invalid hostname).<br/><br/><i>NB
 </i>Use this feature with care as it bypasses the normal certificate verification process",
      "propertyOrder" : 1400,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "authenticationLevel" : {
      "title" : "Authentication Level",
      "description" : "The authentication level associated with this module.<br><br>Each
 authentication module has an authentication level that can be used to indicate the level of security
 associated with the module; 0 is the lowest (and the default). ",
      "propertyOrder" : 1800,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "primaryLdapServer" : {
      "title" : "Primary Active Directory Server ",
      "description" : "Use this list to set the primary Active Directory server used for
 authentication. <br><br>The Active Directory authentication module will use this list as the primary
 server for authentication. A single entry must be in the format:<br/><br/><code>server:port</
code><br/><br/>Multiple entries allow associations between OpenAM servers and an Active Directory
 server. The format is:<br/><br/><code>local server name | server:port</code><br/><br/>The local
 server name is the full name of the server from the list of servers and sites.",
      "propertyOrder" : 100,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "userSearchAttributes" : {
      "title" : "Attributes Used to Search for a User to be Authenticated",
      "description" : "The attributes specified in this list form the LDAP search filter.<br><br>The
 default value of uid will form the following search filter of <code>uid=<i>user</i></code>, if there
```

```
 are multiple values such as uid and cn, the module will create a search filter as follows <code>(|
(uid=<i>user</i>)(cn=<i>user</i>))</code>",
      "propertyOrder" : 700,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "userBindPassword" : {
      "title" : "Bind User Password",
      "description" : "The password of the administration account.",
      "propertyOrder" : 500,
      "required" : true,
      "type" : "string",
      "format" : "password",
      "exampleValue" : ""
    },
    "userSearchFilter" : {
      "title" : "User Search Filter",
      "description" : "This search filter will be appended to the standard user search
 filter.<br><br>This attribute can be used to append a custom search filter to the standard filter.
 For example: <code>(objectClass=person)</code>would result in the following user search filter:<br/
><br/><code>(&(uid=<i>user</i>)(objectClass=person))</code>",
      "propertyOrder" : 800,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "openam-auth-ldap-connection-mode" : {
      "title" : "LDAP Connection Mode",
      "description" : "Defines which protocol/operation is used to establish the connection to the
 LDAP Directory Server.<br><br>If 'LDAP' is selected, the connection <b>won't be secured</b> and
 passwords are transferred in <b>cleartext</b> over the network.<br/> If 'LDAPS' is selected, the
 connection is secured via SSL or TLS. <br/> If 'StartTLS' is selected, the connection is secured by
 using StartTLS extended operation.",
      "propertyOrder" : 1000,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "profileAttributeMappings" : {
      "title" : "User Creation Attributes",
      "description" : "Controls the mapping of local attribute to external attribute for dynamic
 profile creation.<br><br>If dynamic profile creation is enabled; this feature allows for a mapping
 between the attribute/values retrieved from the users authenticated profile and the attribute/values
 that will be provisioned into their matching account in the data store.<br/><br/>The format of this
 property is: <br/><br/><code> local attr1|external attr1</code>",
      "propertyOrder" : 1300,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "connectionHeartbeatTimeUnit" : {
      "title" : "LDAP Connection Heartbeat Time Unit",
```

```
     "description" : "Defines the time unit corresponding to the Heartbeat Interval
setting.<br><br>Use this option in case a firewall/loadbalancer can close idle connections, since the
heartbeat requests will ensure that the connections won't become idle.",
     "propertyOrder" : 1600,
     "required" : true,
     "type" : "string",
     "exampleValue" : ""
   },
   "secondaryLdapServer" : {
     "title" : "Secondary Active Directory Server",
     "description" : "Use this list to set the secondary (failover) Active Directory server used
for authentication.<br><br>If the primary Active Directory server fails, the Active Directory
authentication module will failover to the secondary server. A single entry must be in the
format:<br/><br/><code>server:port</code><br/><br/>Multiple entries allow associations between
OpenAM servers and an Active Directory server. The format is:<br/><br/><code>local server name |
server:port</code><br/><br/><i>NB </i>The local server name is the full name of the server from the
list of servers and sites.",
     "propertyOrder" : 200,
     "required" : true,
     "items" : {
       "type" : "string"
     },
     "type" : "array",
     "exampleValue" : ""
   },
   "userBindDN" : {
     "title" : "Bind User DN",
     "description" : "The DN of an admin user used by the module to authentication to the LDAP
server<br><br>The LDAP module requires an administration account in order to perform functionality
such as password reset.<br/><br/><i>NB </i><code>cn=Directory Manager</code> should not be used in
production systems.",
     "propertyOrder" : 400,
     "required" : true,
     "type" : "string",
     "exampleValue" : ""
   },
   "userProfileRetrievalAttribute" : {
     "title" : "Attribute Used to Retrieve User Profile",
     "description" : "The LDAP module will use this attribute to search of the profile of an
authenticated user.<br><br>This is the attribute used to find the profile of the authenticated user.
Normally this will be the same attribute used to find the user account. The value will be the name of
the user used for authentication.",
     "propertyOrder" : 600,
     "required" : true,
     "type" : "string",
     "exampleValue" : ""
   },
   "connectionHeartbeatInterval" : {
     "title" : "LDAP Connection Heartbeat Interval",
     "description" : "Specifies how often should OpenAM send a heartbeat request to the
directory.<br><br>Use this option in case a firewall/loadbalancer can close idle connections,
since the heartbeat requests will ensure that the connections won't become idle. Use along with the
Heartbeat Time Unit parameter to define the correct interval. Zero or negative value will result in
disabling heartbeat requests.",
     "propertyOrder" : 1500,
     "required" : true,
     "type" : "integer",
     "exampleValue" : ""
   },
```

```
    "userSearchStartDN" : {
      "title" : "DN to Start User Search",
      "description" : "The search for accounts to be authenticated start from this base DN <br><br>For
 a single server just enter the Base DN to be searched. Multiple OpenAM servers can have different
 base DNs for the search The format is as follows:<br/><br/><code>local server name | search DN</
code><br/><br/><i>NB </i>The local server name is the full name of the server from the list of servers
 and sites.",
      "propertyOrder" : 300,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "returnUserDN" : {
      "title" : "Return User DN to DataStore",
      "description" : "Controls whether the DN or the username is returned as the authentication
 principal.",
      "propertyOrder" : 1200,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "searchScope" : {
      "title" : "Search Scope",
      "description" : "The level in the Directory Server that will be searched for a matching
 user profile.<br><br>This attribute controls how the directory is searched.<br/><br/
><ul><li><code>OBJECT</code>: Only the Base DN is searched.</li><li><code>ONELEVEL</code>: Only the
 single level below (and not the Base DN) is searched</li><li><code>SUBTREE</code>: The Base DN and
 all levels below are searched</li></ul>",
      "propertyOrder" : 900,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "operationTimeout" : {
      "title" : "LDAP operations timeout",
      "description" : "Defines the timeout in seconds OpenAM should wait for a response of the
 Directory Server - <code>0</code> means no timeout.<br><br>If the Directory Server's host is down
 completely or the TCP connection became stale OpenAM waits until operation timeouts from the OS or
 the JVM are applied. However this setting allows more granular control within OpenAM itself. A value
 of <code>0</code> means NO timeout is applied on OpenAM level and the timeouts from the JVM or OS
 will apply.",
      "propertyOrder" : 1700,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    }
  }
}
```

delete

Usage:

```
am> delete ActiveDirectoryModule --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action ActiveDirectoryModule --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action ActiveDirectoryModule --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action ActiveDirectoryModule --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query ActiveDirectoryModule --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read ActiveDirectoryModule --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update ActiveDirectoryModule --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "trustAllServerCertificates" : {
      "title" : "Trust All Server Certificates",
      "description" : "Enables a <code>X509TrustManager</code> that trusts all
 certificates.<br><br>This feature will allow the LDAP authentication module to connect to LDAP
 servers protected by self signed or invalid certificates (such as invalid hostname).<br/><br/><i>NB
 </i>Use this feature with care as it bypasses the normal certificate verification process",
      "propertyOrder" : 1400,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "authenticationLevel" : {
      "title" : "Authentication Level",
      "description" : "The authentication level associated with this module.<br><br>Each
 authentication module has an authentication level that can be used to indicate the level of security
 associated with the module; 0 is the lowest (and the default). ",
      "propertyOrder" : 1800,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "primaryLdapServer" : {
      "title" : "Primary Active Directory Server ",
      "description" : "Use this list to set the primary Active Directory server used for
 authentication. <br><br>The Active Directory authentication module will use this list as the primary
 server for authentication. A single entry must be in the format:<br/><br/><code>server:port</
code><br/><br/>Multiple entries allow associations between OpenAM servers and an Active Directory
 server. The format is:<br/><br/><code>local server name | server:port</code><br/><br/>The local
 server name is the full name of the server from the list of servers and sites.",
```

```
      "propertyOrder" : 100,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "userSearchAttributes" : {
      "title" : "Attributes Used to Search for a User to be Authenticated",
      "description" : "The attributes specified in this list form the LDAP search filter.<br><br>The
 default value of uid will form the following search filter of <code>uid=<i>user</i></code>, if there
 are multiple values such as uid and cn, the module will create a search filter as follows <code>(|
(uid=<i>user</i>)(cn=<i>user</i>))</code>",
      "propertyOrder" : 700,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "userBindPassword" : {
      "title" : "Bind User Password",
      "description" : "The password of the administration account.",
      "propertyOrder" : 500,
      "required" : true,
      "type" : "string",
      "format" : "password",
      "exampleValue" : ""
    },
    "userSearchFilter" : {
      "title" : "User Search Filter",
      "description" : "This search filter will be appended to the standard user search
 filter.<br><br>This attribute can be used to append a custom search filter to the standard filter.
 For example: <code>(objectClass=person)</code>would result in the following user search filter:<br/
><br/><code>(&(uid=<i>user</i>)(objectClass=person))</code>",
      "propertyOrder" : 800,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "openam-auth-ldap-connection-mode" : {
      "title" : "LDAP Connection Mode",
      "description" : "Defines which protocol/operation is used to establish the connection to the
 LDAP Directory Server.<br><br>If 'LDAP' is selected, the connection <b>won't be secured</b> and
 passwords are transferred in <b>cleartext</b> over the network.<br/> If 'LDAPS' is selected, the
 connection is secured via SSL or TLS. <br/> If 'StartTLS' is selected, the connection is secured by
 using StartTLS extended operation.",
      "propertyOrder" : 1000,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "profileAttributeMappings" : {
      "title" : "User Creation Attributes",
      "description" : "Controls the mapping of local attribute to external attribute for dynamic
 profile creation.<br><br>If dynamic profile creation is enabled; this feature allows for a mapping
 between the attribute/values retrieved from the users authenticated profile and the attribute/values
```

```
that will be provisioned into their matching account in the data store.<br/><br/>The format of this
property is: <br/><br/><code> local attr1|external attr1</code>",
     "propertyOrder" : 1300,
     "required" : true,
     "items" : {
       "type" : "string"
     },
     "type" : "array",
     "exampleValue" : ""
   },
   "connectionHeartbeatTimeUnit" : {
     "title" : "LDAP Connection Heartbeat Time Unit",
     "description" : "Defines the time unit corresponding to the Heartbeat Interval
setting.<br><br>Use this option in case a firewall/loadbalancer can close idle connections, since the
heartbeat requests will ensure that the connections won't become idle.",
     "propertyOrder" : 1600,
     "required" : true,
     "type" : "string",
     "exampleValue" : ""
   },
   "secondaryLdapServer" : {
     "title" : "Secondary Active Directory Server",
     "description" : "Use this list to set the secondary (failover) Active Directory server used
for authentication.<br><br>If the primary Active Directory server fails, the Active Directory
authentication module will failover to the secondary server. A single entry must be in the
format:<br/><br/><code>server:port</code><br/><br/>Multiple entries allow associations between
OpenAM servers and an Active Directory server. The format is:<br/><br/><code>local server name |
server:port</code><br/><br/><i>NB </i>The local server name is the full name of the server from the
list of servers and sites.",
     "propertyOrder" : 200,
     "required" : true,
     "items" : {
       "type" : "string"
     },
     "type" : "array",
     "exampleValue" : ""
   },
   "userBindDN" : {
     "title" : "Bind User DN",
     "description" : "The DN of an admin user used by the module to authentication to the LDAP
server<br><br>The LDAP module requires an administration account in order to perform functionality
such as password reset.<br/><br/><i>NB </i><code>cn=Directory Manager</code> should not be used in
production systems.",
     "propertyOrder" : 400,
     "required" : true,
     "type" : "string",
     "exampleValue" : ""
   },
   "userProfileRetrievalAttribute" : {
     "title" : "Attribute Used to Retrieve User Profile",
     "description" : "The LDAP module will use this attribute to search of the profile of an
authenticated user.<br><br>This is the attribute used to find the profile of the authenticated user.
Normally this will be the same attribute used to find the user account. The value will be the name of
the user used for authentication.",
     "propertyOrder" : 600,
     "required" : true,
     "type" : "string",
     "exampleValue" : ""
   },
```

```
    "connectionHeartbeatInterval" : {
      "title" : "LDAP Connection Heartbeat Interval",
      "description" : "Specifies how often should OpenAM send a heartbeat request to the
 directory.<br><br>Use this option in case a firewall/loadbalancer can close idle connections,
 since the heartbeat requests will ensure that the connections won't become idle. Use along with the
 Heartbeat Time Unit parameter to define the correct interval. Zero or negative value will result in
 disabling heartbeat requests.",
      "propertyOrder" : 1500,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "userSearchStartDN" : {
      "title" : "DN to Start User Search",
      "description" : "The search for accounts to be authenticated start from this base DN <br><br>For
 a single server just enter the Base DN to be searched. Multiple OpenAM servers can have different
 base DNs for the search The format is as follows:<br/><br/><code>local server name | search DN</
code><br/><br/><i>NB </i>The local server name is the full name of the server from the list of servers
 and sites.",
      "propertyOrder" : 300,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "returnUserDN" : {
      "title" : "Return User DN to DataStore",
      "description" : "Controls whether the DN or the username is returned as the authentication
 principal.",
      "propertyOrder" : 1200,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "searchScope" : {
      "title" : "Search Scope",
      "description" : "The level in the Directory Server that will be searched for a matching
 user profile.<br><br>This attribute controls how the directory is searched.<br/><br/
><ul><li><code>OBJECT</code>: Only the Base DN is searched.</li><li><code>ONELEVEL</code>: Only the
 single level below (and not the Base DN) is searched</li><li><code>SUBTREE</code>: The Base DN and
 all levels below are searched</li></ul>",
      "propertyOrder" : 900,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "operationTimeout" : {
      "title" : "LDAP operations timeout",
      "description" : "Defines the timeout in seconds OpenAM should wait for a response of the
 Directory Server - <code>0</code> means no timeout.<br><br>If the Directory Server's host is down
 completely or the TCP connection became stale OpenAM waits until operation timeouts from the OS or
 the JVM are applied. However this setting allows more granular control within OpenAM itself. A value
 of <code>0</code> means NO timeout is applied on OpenAM level and the timeouts from the JVM or OS
 will apply.",
      "propertyOrder" : 1700,
      "required" : true,
      "type" : "integer",
```

```
      "exampleValue" : ""
    }
  }
}
```

Global Operations

Resource path: `/global-config/authentication/modules/activedirectory`

Resource version: `1.0`

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action ActiveDirectoryModule --global --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action ActiveDirectoryModule --global --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action ActiveDirectoryModule --global --actionName nextdescendents
```

read

Usage:

```
am> read ActiveDirectoryModule --global
```

update

Usage:

```
am> update ActiveDirectoryModule --global --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "defaults" : {
      "properties" : {
        "userSearchFilter" : {
          "title" : "User Search Filter",
          "description" : "This search filter will be appended to the standard user search
 filter.<br><br>This attribute can be used to append a custom search filter to the standard filter.
 For example: <code>(objectClass=person)</code>would result in the following user search filter:<br/
><br/><code>(&(uid=<i>user</i>)(objectClass=person))</code>",
          "propertyOrder" : 800,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "connectionHeartbeatTimeUnit" : {
          "title" : "LDAP Connection Heartbeat Time Unit",
          "description" : "Defines the time unit corresponding to the Heartbeat Interval
 setting.<br><br>Use this option in case a firewall/loadbalancer can close idle connections, since the
 heartbeat requests will ensure that the connections won't become idle.",
          "propertyOrder" : 1600,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "operationTimeout" : {
          "title" : "LDAP operations timeout",
          "description" : "Defines the timeout in seconds OpenAM should wait for a response of the
 Directory Server - <code>0</code> means no timeout.<br><br>If the Directory Server's host is down
 completely or the TCP connection became stale OpenAM waits until operation timeouts from the OS or
 the JVM are applied. However this setting allows more granular control within OpenAM itself. A value
 of <code>0</code> means NO timeout is applied on OpenAM level and the timeouts from the JVM or OS
 will apply.",
          "propertyOrder" : 1700,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "primaryLdapServer" : {
          "title" : "Primary Active Directory Server ",
          "description" : "Use this list to set the primary Active Directory server used for
 authentication. <br><br>The Active Directory authentication module will use this list as the primary
 server for authentication. A single entry must be in the format:<br/><br/><code>server:port</
code><br/><br/>Multiple entries allow associations between OpenAM servers and an Active Directory
 server. The format is:<br/><br/><code>local server name | server:port</code><br/><br/>The local
 server name is the full name of the server from the list of servers and sites.",
          "propertyOrder" : 100,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
```

```
        "exampleValue" : ""
      },
      "openam-auth-ldap-connection-mode" : {
        "title" : "LDAP Connection Mode",
        "description" : "Defines which protocol/operation is used to establish the connection to
the LDAP Directory Server.<br><br>If 'LDAP' is selected, the connection <b>won't be secured</b> and
passwords are transferred in <b>cleartext</b> over the network.<br/> If 'LDAPS' is selected, the
connection is secured via SSL or TLS. <br/> If 'StartTLS' is selected, the connection is secured by
using StartTLS extended operation.",
        "propertyOrder" : 1000,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
      },
      "returnUserDN" : {
        "title" : "Return User DN to DataStore",
        "description" : "Controls whether the DN or the username is returned as the authentication
principal.",
        "propertyOrder" : 1200,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
      },
      "connectionHeartbeatInterval" : {
        "title" : "LDAP Connection Heartbeat Interval",
        "description" : "Specifies how often should OpenAM send a heartbeat request to the
directory.<br><br>Use this option in case a firewall/loadbalancer can close idle connections,
since the heartbeat requests will ensure that the connections won't become idle. Use along with the
Heartbeat Time Unit parameter to define the correct interval. Zero or negative value will result in
disabling heartbeat requests.",
        "propertyOrder" : 1500,
        "required" : true,
        "type" : "integer",
        "exampleValue" : ""
      },
      "userSearchStartDN" : {
        "title" : "DN to Start User Search",
        "description" : "The search for accounts to be authenticated start from this base DN
<br><br>For a single server just enter the Base DN to be searched. Multiple OpenAM servers can have
different base DNs for the search The format is as follows:<br/><br/><code>local server name | search
DN</code><br/><br/><i>NB </i>The local server name is the full name of the server from the list of
servers and sites.",
        "propertyOrder" : 300,
        "required" : true,
        "items" : {
          "type" : "string"
        },
        "type" : "array",
        "exampleValue" : ""
      },
      "secondaryLdapServer" : {
        "title" : "Secondary Active Directory Server",
        "description" : "Use this list to set the secondary (failover) Active Directory server
used for authentication.<br><br>If the primary Active Directory server fails, the Active Directory
authentication module will failover to the secondary server. A single entry must be in the
format:<br/><br/><code>server:port</code><br/><br/>Multiple entries allow associations between
OpenAM servers and an Active Directory server. The format is:<br/><br/><code>local server name |
server:port</code><br/><br/><i>NB </i>The local server name is the full name of the server from the
list of servers and sites.",
```

```
          "propertyOrder" : 200,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "trustAllServerCertificates" : {
          "title" : "Trust All Server Certificates",
          "description" : "Enables a <code>X509TrustManager</code> that trusts all
 certificates.<br><br>This feature will allow the LDAP authentication module to connect to LDAP
 servers protected by self signed or invalid certificates (such as invalid hostname).<br/><br/><i>NB
 </i>Use this feature with care as it bypasses the normal certificate verification process",
          "propertyOrder" : 1400,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "profileAttributeMappings" : {
          "title" : "User Creation Attributes",
          "description" : "Controls the mapping of local attribute to external attribute for dynamic
 profile creation.<br><br>If dynamic profile creation is enabled; this feature allows for a mapping
 between the attribute/values retrieved from the users authenticated profile and the attribute/values
 that will be provisioned into their matching account in the data store.<br/><br/>The format of this
 property is: <br/><br/><code> local attr1|external attr1</code>",
          "propertyOrder" : 1300,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "userSearchAttributes" : {
          "title" : "Attributes Used to Search for a User to be Authenticated",
          "description" : "The attributes specified in this list form the LDAP search
 filter.<br><br>The default value of uid will form the following search filter of <code>uid=<i>user</
i></code>, if there are multiple values such as uid and cn, the module will create a search filter as
 follows <code>(|(uid=<i>user</i>)(cn=<i>user</i>))</code>",
          "propertyOrder" : 700,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "userProfileRetrievalAttribute" : {
          "title" : "Attribute Used to Retrieve User Profile",
          "description" : "The LDAP module will use this attribute to search of the profile of an
 authenticated user.<br><br>This is the attribute used to find the profile of the authenticated user.
 Normally this will be the same attribute used to find the user account. The value will be the name of
 the user used for authentication.",
          "propertyOrder" : 600,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
```

```
        "authenticationLevel" : {
          "title" : "Authentication Level",
          "description" : "The authentication level associated with this module.<br><br>Each
 authentication module has an authentication level that can be used to indicate the level of security
 associated with the module; 0 is the lowest (and the default). ",
          "propertyOrder" : 1800,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "searchScope" : {
          "title" : "Search Scope",
          "description" : "The level in the Directory Server that will be searched for a
 matching user profile.<br><br>This attribute controls how the directory is searched.<br/><br/
><ul><li><code>OBJECT</code>: Only the Base DN is searched.</li><li><code>ONELEVEL</code>: Only the
 single level below (and not the Base DN) is searched</li><li><code>SUBTREE</code>: The Base DN and
 all levels below are searched</li></ul>",
          "propertyOrder" : 900,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "userBindDN" : {
          "title" : "Bind User DN",
          "description" : "The DN of an admin user used by the module to authentication to the LDAP
 server<br><br>The LDAP module requires an administration account in order to perform functionality
 such as password reset.<br/><br/><i>NB </i><code>cn=Directory Manager</code> should not be used in
 production systems.",
          "propertyOrder" : 400,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "userBindPassword" : {
          "title" : "Bind User Password",
          "description" : "The password of the administration account.",
          "propertyOrder" : 500,
          "required" : true,
          "type" : "string",
          "format" : "password",
          "exampleValue" : ""
        }
      },
      "type" : "object",
      "title" : "Realm Defaults"
    }
  }
}
```

AdaptiveRiskModule

Realm Operations

Resource path: `/realm-config/authentication/modules/adaptiverisk`

Resource version: `1.0`

create

Usage:

```
am> create AdaptiveRiskModule --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "attributecheck" : {
      "type" : "object",
      "title" : "Profile Attribute",
      "propertyOrder" : 7,
      "properties" : {
        "profileRiskAttributeCheckEnabled" : {
          "title" : "Profile Risk Attribute check",
          "description" : "Enables the checking of the user profile for a matching attribute and
 value.<br><br>If this check is enabled, the check will pass if the users profile contains the
 required risk attribute and value.",
          "propertyOrder" : 2800,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "profileRiskAttributeName" : {
          "title" : "Attribute Name",
          "description" : "The name of the attribute to retrieve from the user profile in the data
 store.",
          "propertyOrder" : 2900,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "profileRiskAttributeScore" : {
          "title" : "Score",
          "description" : "The amount to increment the score if this check fails.",
          "propertyOrder" : 3100,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "invertProfileRiskAttributeScore" : {
```

```
          "title" : "Invert Result",
          "description" : "If the check succeeds the score will be included in the total, for failure
the score will not be incremented.",
          "propertyOrder" : 3200,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "profileRiskAttributeValue" : {
          "title" : "Attribute Value",
          "description" : "The required value of the named attribute.",
          "propertyOrder" : 3000,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "iphistory" : {
      "type" : "object",
      "title" : "IP Address History",
      "propertyOrder" : 3,
      "properties" : {
        "ipHistoryScore" : {
          "title" : "Score",
          "description" : "The amount to increment the score if this check fails.",
          "propertyOrder" : 1400,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "invertIPHistoryScore" : {
          "title" : "Invert Result",
          "description" : "If the check succeeds the score will be included in the total, for failure
the score will not be incremented.",
          "propertyOrder" : 1500,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "ipHistoryCheckEnabled" : {
          "title" : "IP History Check",
          "description" : "Enables the checking of client IP address against a list of past IP
addresses.<br><br>If this check is enabled; a set number of past IP addresses used by the client to
access OpenAM is recorded in the user profile. This check passes if the current client IP address
is present in the history list. If the IP address is not present, the check fails and the IP address
is added to list if the overall authentication is successful (causing the oldest IP address to be
removed).",
          "propertyOrder" : 1000,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "ipHistoryProfileAttribute" : {
          "title" : "Profile Attribute Name",
          "description" : "The name of the attribute used to store the IP history list in the data
store.<br><br>IP history list is stored in the Data Store meaning your Data Store should be able
to store values under the configured attribute name. If you're using a directory server as backend,
```

```
make sure your Data Store configuration contains the necessary objectclass and attribute related
settings.",
         "propertyOrder" : 1200,
         "required" : true,
         "type" : "string",
         "exampleValue" : ""
       },
       "saveSuccessfulIP" : {
         "title" : "Save Successful IP Address",
         "description" : "The IP History list will be updated in the data store<br><br>The Adaptive
Risk Post Authentication Plug-in will update the IP history list if the overall authentication is
successful.",
         "propertyOrder" : 1300,
         "required" : true,
         "type" : "boolean",
         "exampleValue" : ""
       },
       "ipHistoryCount" : {
         "title" : "History size",
         "description" : "The number of client IP addresses to save in the history list.",
         "propertyOrder" : 1100,
         "required" : true,
         "type" : "integer",
         "exampleValue" : ""
       }
     }
   },
   "knowncookie" : {
     "type" : "object",
     "title" : "Known Cookie",
     "propertyOrder" : 4,
     "properties" : {
       "knownCookieCheckEnabled" : {
         "title" : "Cookie Value Check",
         "description" : "Enables the checking of a known cookie value in the client
request<br><br>If this check is enabled, the check looks for a known cookie in the client request. If
the cookie exists and has the correct value then the check will pass. ",
         "propertyOrder" : 1600,
         "required" : true,
         "type" : "boolean",
         "exampleValue" : ""
       },
       "knownCookieScore" : {
         "title" : "Score",
         "description" : "The amount to increment the score if this check fails.",
         "propertyOrder" : 2000,
         "required" : true,
         "type" : "integer",
         "exampleValue" : ""
       },
       "createKnownCookieOnSuccessfulLogin" : {
         "title" : "Save Cookie Value on Successful Login",
         "description" : "The cookie will be created on the client after successful login<br><br>The
Adaptive Risk Post Authentication Plug-in will set the cookie on the client response",
         "propertyOrder" : 1900,
         "required" : true,
         "type" : "boolean",
         "exampleValue" : ""
       },
```

```
        "knownCookieName" : {
          "title" : "Cookie Name",
          "description" : "The name of the cookie to set on the client.",
          "propertyOrder" : 1700,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "invertKnownCookieScore" : {
          "title" : "Invert Result",
          "description" : "If the check succeeds the score will be included in the total, for failure
 the score will not be incremented.",
          "propertyOrder" : 2100,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "knownCookieValue" : {
          "title" : "Cookie Value",
          "description" : "The value to be set on the cookie.",
          "propertyOrder" : 1800,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "iprange" : {
      "type" : "object",
      "title" : "IP Address Range",
      "propertyOrder" : 2,
      "properties" : {
        "ipRangeCheckEnabled" : {
          "title" : "IP Range Check",
          "description" : "Enables the checking of the client IP address against a list of IP
 addresses.<br><br>The IP range check compares the IP of the client against a list of IP addresses, if
 the client IP is found within said list the check is successful.",
          "propertyOrder" : 600,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "ipRange" : {
          "title" : "IP Range",
          "description" : "The list of IP address to compare against the client IP address.<br><br>The
 format of the IP address is as follows:<br/><br/><ul><li>Single IP address: <code>172.16.90.1</
code></li><li>CIDR notation: <code>172.16.90.0/24</code></li><li>IP net-block with netmask:
 <code>172.16.90.0:255.255.255.0</code></li></ul>",
          "propertyOrder" : 700,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "ipRangeScore" : {
          "title" : "Score",
          "description" : "The amount to increment the score if this check fails.",
```

```
          "propertyOrder" : 800,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "invertIPRangeScoreEnabled" : {
          "title" : "Invert Result",
          "description" : "If the check succeeds the score will be included in the total, for failure
the score will not be incremented.",
          "propertyOrder" : 900,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        }
      }
    },
    "requestheader" : {
      "type" : "object",
      "title" : "Request Header",
      "propertyOrder" : 9,
      "properties" : {
        "requestHeaderValue" : {
          "title" : "Request Header Value",
          "description" : "The required value of the named HTTP header.",
          "propertyOrder" : 4500,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "invertRequestHeaderScore" : {
          "title" : "Invert Result",
          "description" : "If the check succeeds the score will be included in the total, for failure
the score will not be incremented.",
          "propertyOrder" : 4700,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "requestHeaderScore" : {
          "title" : "Score",
          "description" : "The amount to increment the score if this check fails.",
          "propertyOrder" : 4600,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "requestHeaderCheckEnabled" : {
          "title" : "Request Header Check",
          "description" : "Enables the checking of the client request for a known header name and
value.<br><br>The request header check will pass if the client request contains the required named
header and value.",
          "propertyOrder" : 4300,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "requestHeaderName" : {
          "title" : "Request Header Name",
          "description" : "The name of the required HTTP header ",
```

```
          "propertyOrder" : 4400,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "lastlogin" : {
      "type" : "object",
      "title" : "Time Since Last Login",
      "propertyOrder" : 6,
      "properties" : {
        "timeSinceLastLoginCookieName" : {
          "title" : "Cookie Name",
          "description" : "The name of the cookie used to store the time of the last successful
authentication.",
          "propertyOrder" : 2300,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "maxTimeSinceLastLogin" : {
          "title" : "Max Time since Last login",
          "description" : "The maximum number of days that can elapse before this test.",
          "propertyOrder" : 2400,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "saveLastLoginTimeOnSuccessfulLogin" : {
          "title" : "Save time of Successful Login",
          "description" : "The last login time will be saved in a client cookie<br><br>The Adaptive
Risk Post Authentication Plug-in will update the last login time",
          "propertyOrder" : 2500,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "invertTimeSinceLastLoginScore" : {
          "title" : "Invert Result",
          "description" : "If the check succeeds the score will be included in the total, for failure
the score will not be incremented.",
          "propertyOrder" : 2700,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "timeSinceLastLoginScore" : {
          "title" : "Score",
          "description" : "The amount to increment the score if this check fails.",
          "propertyOrder" : 2600,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "timeSinceLastLoginCheckEnabled" : {
          "title" : "Time since Last login Check",
          "description" : "Enables the checking of the last time the user successfully
authenticated.<br><br>If this check is enabled, the check ensures the user has successfully
```

```
authenticated within a given interval. If the interval has been exceeded the check will fail. The
last authentication for the user is stored in a client cookie.",
         "propertyOrder" : 2200,
         "required" : true,
         "type" : "boolean",
         "exampleValue" : ""
       }
     }
   },
   "devicecookie" : {
     "type" : "object",
     "title" : "Device Cookie",
     "propertyOrder" : 5,
     "properties" : {
       "invertDeviceCookieScore" : {
         "title" : "Invert Result",
         "description" : "If the check succeeds the score will be included in the total, for failure
the score will not be incremented.",
         "propertyOrder" : 3700,
         "required" : true,
         "type" : "boolean",
         "exampleValue" : ""
       },
       "saveDeviceCookieValueOnSuccessfulLogin" : {
         "title" : "Save Device Registration on Successful Login",
         "description" : "Set the device cookie on the client response<br><br>The Adaptive Risk Post
Authentication Plug-in will set the device cookie on the client response",
         "propertyOrder" : 3500,
         "required" : true,
         "type" : "boolean",
         "exampleValue" : ""
       },
       "deviceCookieName" : {
         "title" : "Cookie Name",
         "description" : "The name of the cookie to be checked for (and optionally set) on the client
request",
         "propertyOrder" : 3400,
         "required" : true,
         "type" : "string",
         "exampleValue" : ""
       },
       "deviceCookieCheckEnabled" : {
         "title" : "Device Registration Cookie Check",
         "description" : "Enables the checking of the client request for a known cookie.<br><br>If
this check is enabled, the check will pass if the client request contains the named cookie.",
         "propertyOrder" : 3300,
         "required" : true,
         "type" : "boolean",
         "exampleValue" : ""
       },
       "deviceCookieScore" : {
         "title" : "Score",
         "description" : "The amount to increment the score if this check fails.",
         "propertyOrder" : 3600,
         "required" : true,
         "type" : "integer",
         "exampleValue" : ""
       }
     }
```

```
    },
    "geolocation" : {
      "type" : "object",
      "title" : "Geo Location",
      "propertyOrder" : 8,
      "properties" : {
        "geolocationValidCountryCodes" : {
          "title" : "Valid Country Codes",
          "description" : "The list of country codes that are considered as valid locations for client
 IPs.<br><br>The list is made up of country codes separated by a | character; for example:<br/><br/
><code>gb|us|no|fr</code>",
          "propertyOrder" : 4000,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "geolocationCheckEnabled" : {
          "title" : "Geolocation Country Code Check",
          "description" : "Enables the checking of the client IP address against the geolocation
 database.<br><br>The geolocation database associates IP addresses against their known location. This
 check passes if the country associated with the client IP address is matched against the list of
 valid country codes.<br/><br/>The geolocation database is available in binary format at <a href=
\"http://www.maxmind.com/app/country\" target=\"_blank\">MaxMind</a>.",
          "propertyOrder" : 3800,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "geolocationScore" : {
          "title" : "Score",
          "description" : "The amount to increment the score if this check fails.",
          "propertyOrder" : 4100,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "invertGeolocationScore" : {
          "title" : "Invert Result",
          "description" : "If the check succeeds the score will be included in the total, for failure
 the score will not be incremented.",
          "propertyOrder" : 4200,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "geolocationDatabaseLocation" : {
          "title" : "Geolocation Database location",
          "description" : "The path to the location of the GEO location database.<br><br>The
 Geolocation database is not distributed with OpenAM, you can get it in binary format from <a href=
\"http://www.maxmind.com/app/country\" target=\"_blank\">MaxMind</a>.",
          "propertyOrder" : 3900,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "general" : {
      "type" : "object",
```

```
      "title" : "General",
      "propertyOrder" : 0,
      "properties" : {
        "authenticationLevel" : {
          "title" : "Authentication Level",
          "description" : "The authentication level associated with this module.<br><br>Each
 authentication module has an authentication level that can be used to indicate the level of security
 associated with the module; 0 is the lowest (and the default).",
          "propertyOrder" : 100,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "riskThreshold" : {
          "title" : "Risk Threshold",
          "description" : "If the risk threshold value is not reached after executing the different
 tests, the authentication is considered to be successful.<br><br>Associated with many of the adaptive
 risk checks is a score; if a check does not passes then the score is added to the current running
 total. The final score is then compared with the <i>Risk Threshold</i>, if the score is lesser than
 said threshold the module will be successful. ",
          "propertyOrder" : 200,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        }
      }
    },
    "authfailed" : {
      "type" : "object",
      "title" : "Failed Authentications",
      "propertyOrder" : 1,
      "properties" : {
        "failureScore" : {
          "title" : "Score",
          "description" : "The amount to increment the score if this check fails.",
          "propertyOrder" : 400,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "invertFailureScore" : {
          "title" : "Invert Result",
          "description" : "If the check succeeds the score will be included in the total, for failure
 the score will not be incremented.",
          "propertyOrder" : 500,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "failedAuthenticationCheckEnabled" : {
          "title" : "Failed Authentication Check",
          "description" : "Checks if the user has past authentication failures.<br><br>Check if the
 OpenAM account lockout mechanism has recorded past authentication failures for the user.<br/><br/
><i>NB </i>For this check to function, Account Lockout must be enabled.",
          "propertyOrder" : 300,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        }
```

```
      }
    }
  }
}
```

delete

Usage:

```
am> delete AdaptiveRiskModule --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action AdaptiveRiskModule --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action AdaptiveRiskModule --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action AdaptiveRiskModule --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query AdaptiveRiskModule --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read AdaptiveRiskModule --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update AdaptiveRiskModule --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "attributecheck" : {
      "type" : "object",
      "title" : "Profile Attribute",
      "propertyOrder" : 7,
      "properties" : {
        "profileRiskAttributeCheckEnabled" : {
          "title" : "Profile Risk Attribute check",
          "description" : "Enables the checking of the user profile for a matching attribute and
 value.<br><br>If this check is enabled, the check will pass if the users profile contains the
 required risk attribute and value.",
          "propertyOrder" : 2800,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "profileRiskAttributeName" : {
          "title" : "Attribute Name",
          "description" : "The name of the attribute to retrieve from the user profile in the data
 store.",
```

```
          "propertyOrder" : 2900,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "profileRiskAttributeScore" : {
          "title" : "Score",
          "description" : "The amount to increment the score if this check fails.",
          "propertyOrder" : 3100,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "invertProfileRiskAttributeScore" : {
          "title" : "Invert Result",
          "description" : "If the check succeeds the score will be included in the total, for failure
the score will not be incremented.",
          "propertyOrder" : 3200,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "profileRiskAttributeValue" : {
          "title" : "Attribute Value",
          "description" : "The required value of the named attribute.",
          "propertyOrder" : 3000,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "iphistory" : {
      "type" : "object",
      "title" : "IP Address History",
      "propertyOrder" : 3,
      "properties" : {
        "ipHistoryScore" : {
          "title" : "Score",
          "description" : "The amount to increment the score if this check fails.",
          "propertyOrder" : 1400,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "invertIPHistoryScore" : {
          "title" : "Invert Result",
          "description" : "If the check succeeds the score will be included in the total, for failure
the score will not be incremented.",
          "propertyOrder" : 1500,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "ipHistoryCheckEnabled" : {
          "title" : "IP History Check",
          "description" : "Enables the checking of client IP address against a list of past IP
addresses.<br><br>If this check is enabled; a set number of past IP addresses used by the client to
access OpenAM is recorded in the user profile. This check passes if the current client IP address
```

```
is present in the history list. If the IP address is not present, the check fails and the IP address
is added to list if the overall authentication is successful (causing the oldest IP address to be
removed).",
          "propertyOrder" : 1000,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "ipHistoryProfileAttribute" : {
          "title" : "Profile Attribute Name",
          "description" : "The name of the attribute used to store the IP history list in the data
store.<br><br>IP history list is stored in the Data Store meaning your Data Store should be able
to store values under the configured attribute name. If you're using a directory server as backend,
make sure your Data Store configuration contains the necessary objectclass and attribute related
settings.",
          "propertyOrder" : 1200,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "saveSuccessfulIP" : {
          "title" : "Save Successful IP Address",
          "description" : "The IP History list will be updated in the data store<br><br>The Adaptive
Risk Post Authentication Plug-in will update the IP history list if the overall authentication is
successful.",
          "propertyOrder" : 1300,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "ipHistoryCount" : {
          "title" : "History size",
          "description" : "The number of client IP addresses to save in the history list.",
          "propertyOrder" : 1100,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        }
      }
    },
    "knowncookie" : {
      "type" : "object",
      "title" : "Known Cookie",
      "propertyOrder" : 4,
      "properties" : {
        "knownCookieCheckEnabled" : {
          "title" : "Cookie Value Check",
          "description" : "Enables the checking of a known cookie value in the client
request<br><br>If this check is enabled, the check looks for a known cookie in the client request. If
the cookie exists and has the correct value then the check will pass. ",
          "propertyOrder" : 1600,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "knownCookieScore" : {
          "title" : "Score",
          "description" : "The amount to increment the score if this check fails.",
          "propertyOrder" : 2000,
```

```
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "createKnownCookieOnSuccessfulLogin" : {
          "title" : "Save Cookie Value on Successful Login",
          "description" : "The cookie will be created on the client after successful login<br><br>The
Adaptive Risk Post Authentication Plug-in will set the cookie on the client response",
          "propertyOrder" : 1900,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "knownCookieName" : {
          "title" : "Cookie Name",
          "description" : "The name of the cookie to set on the client.",
          "propertyOrder" : 1700,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "invertKnownCookieScore" : {
          "title" : "Invert Result",
          "description" : "If the check succeeds the score will be included in the total, for failure
the score will not be incremented.",
          "propertyOrder" : 2100,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "knownCookieValue" : {
          "title" : "Cookie Value",
          "description" : "The value to be set on the cookie.",
          "propertyOrder" : 1800,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "iprange" : {
      "type" : "object",
      "title" : "IP Address Range",
      "propertyOrder" : 2,
      "properties" : {
        "ipRangeCheckEnabled" : {
          "title" : "IP Range Check",
          "description" : "Enables the checking of the client IP address against a list of IP
addresses.<br><br>The IP range check compares the IP of the client against a list of IP addresses, if
the client IP is found within said list the check is successful.",
          "propertyOrder" : 600,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "ipRange" : {
          "title" : "IP Range",
          "description" : "The list of IP address to compare against the client IP address.<br><br>The
format of the IP address is as follows:<br/><br/><ul><li>Single IP address: <code>172.16.90.1</
```

```
code></li><li>CIDR notation: <code>172.16.90.0/24</code></li><li>IP net-block with netmask:
 <code>172.16.90.0:255.255.255.0</code></li></ul>",
          "propertyOrder" : 700,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "ipRangeScore" : {
          "title" : "Score",
          "description" : "The amount to increment the score if this check fails.",
          "propertyOrder" : 800,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "invertIPRangeScoreEnabled" : {
          "title" : "Invert Result",
          "description" : "If the check succeeds the score will be included in the total, for failure
 the score will not be incremented.",
          "propertyOrder" : 900,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        }
      }
    },
    "requestheader" : {
      "type" : "object",
      "title" : "Request Header",
      "propertyOrder" : 9,
      "properties" : {
        "requestHeaderValue" : {
          "title" : "Request Header Value",
          "description" : "The required value of the named HTTP header.",
          "propertyOrder" : 4500,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "invertRequestHeaderScore" : {
          "title" : "Invert Result",
          "description" : "If the check succeeds the score will be included in the total, for failure
 the score will not be incremented.",
          "propertyOrder" : 4700,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "requestHeaderScore" : {
          "title" : "Score",
          "description" : "The amount to increment the score if this check fails.",
          "propertyOrder" : 4600,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
```

```
       "requestHeaderCheckEnabled" : {
         "title" : "Request Header Check",
         "description" : "Enables the checking of the client request for a known header name and
value.<br><br>The request header check will pass if the client request contains the required named
header and value.",
         "propertyOrder" : 4300,
         "required" : true,
         "type" : "boolean",
         "exampleValue" : ""
       },
       "requestHeaderName" : {
         "title" : "Request Header Name",
         "description" : "The name of the required HTTP header ",
         "propertyOrder" : 4400,
         "required" : true,
         "type" : "string",
         "exampleValue" : ""
       }
     }
   },
   "lastlogin" : {
     "type" : "object",
     "title" : "Time Since Last Login",
     "propertyOrder" : 6,
     "properties" : {
       "timeSinceLastLoginCookieName" : {
         "title" : "Cookie Name",
         "description" : "The name of the cookie used to store the time of the last successful
authentication.",
         "propertyOrder" : 2300,
         "required" : true,
         "type" : "string",
         "exampleValue" : ""
       },
       "maxTimeSinceLastLogin" : {
         "title" : "Max Time since Last login",
         "description" : "The maximum number of days that can elapse before this test.",
         "propertyOrder" : 2400,
         "required" : true,
         "type" : "string",
         "exampleValue" : ""
       },
       "saveLastLoginTimeOnSuccessfulLogin" : {
         "title" : "Save time of Successful Login",
         "description" : "The last login time will be saved in a client cookie<br><br>The Adaptive
Risk Post Authentication Plug-in will update the last login time",
         "propertyOrder" : 2500,
         "required" : true,
         "type" : "boolean",
         "exampleValue" : ""
       },
       "invertTimeSinceLastLoginScore" : {
         "title" : "Invert Result",
         "description" : "If the check succeeds the score will be included in the total, for failure
the score will not be incremented.",
         "propertyOrder" : 2700,
         "required" : true,
         "type" : "boolean",
         "exampleValue" : ""
```

```
       },
       "timeSinceLastLoginScore" : {
         "title" : "Score",
         "description" : "The amount to increment the score if this check fails.",
         "propertyOrder" : 2600,
         "required" : true,
         "type" : "integer",
         "exampleValue" : ""
       },
       "timeSinceLastLoginCheckEnabled" : {
         "title" : "Time since Last login Check",
         "description" : "Enables the checking of the last time the user successfully
authenticated.<br><br>If this check is enabled, the check ensures the user has successfully
authenticated within a given interval. If the interval has been exceeded the check will fail. The
last authentication for the user is stored in a client cookie.",
         "propertyOrder" : 2200,
         "required" : true,
         "type" : "boolean",
         "exampleValue" : ""
       }
     }
   },
   "devicecookie" : {
     "type" : "object",
     "title" : "Device Cookie",
     "propertyOrder" : 5,
     "properties" : {
       "invertDeviceCookieScore" : {
         "title" : "Invert Result",
         "description" : "If the check succeeds the score will be included in the total, for failure
the score will not be incremented.",
         "propertyOrder" : 3700,
         "required" : true,
         "type" : "boolean",
         "exampleValue" : ""
       },
       "saveDeviceCookieValueOnSuccessfulLogin" : {
         "title" : "Save Device Registration on Successful Login",
         "description" : "Set the device cookie on the client response<br><br>The Adaptive Risk Post
Authentication Plug-in will set the device cookie on the client response",
         "propertyOrder" : 3500,
         "required" : true,
         "type" : "boolean",
         "exampleValue" : ""
       },
       "deviceCookieName" : {
         "title" : "Cookie Name",
         "description" : "The name of the cookie to be checked for (and optionally set) on the client
request",
         "propertyOrder" : 3400,
         "required" : true,
         "type" : "string",
         "exampleValue" : ""
       },
       "deviceCookieCheckEnabled" : {
         "title" : "Device Registration Cookie Check",
         "description" : "Enables the checking of the client request for a known cookie.<br><br>If
this check is enabled, the check will pass if the client request contains the named cookie.",
         "propertyOrder" : 3300,
```

```
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "deviceCookieScore" : {
          "title" : "Score",
          "description" : "The amount to increment the score if this check fails.",
          "propertyOrder" : 3600,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        }
      }
    },
    "geolocation" : {
      "type" : "object",
      "title" : "Geo Location",
      "propertyOrder" : 8,
      "properties" : {
        "geolocationValidCountryCodes" : {
          "title" : "Valid Country Codes",
          "description" : "The list of country codes that are considered as valid locations for client
 IPs.<br><br>The list is made up of country codes separated by a | character; for example:<br/><br/
><code>gb|us|no|fr</code>",
          "propertyOrder" : 4000,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "geolocationCheckEnabled" : {
          "title" : "Geolocation Country Code Check",
          "description" : "Enables the checking of the client IP address against the geolocation
 database.<br><br>The geolocation database associates IP addresses against their known location. This
 check passes if the country associated with the client IP address is matched against the list of
 valid country codes.<br/><br/>The geolocation database is available in binary format at <a href=
\"http://www.maxmind.com/app/country\" target=\"_blank\">MaxMind</a>.",
          "propertyOrder" : 3800,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "geolocationScore" : {
          "title" : "Score",
          "description" : "The amount to increment the score if this check fails.",
          "propertyOrder" : 4100,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "invertGeolocationScore" : {
          "title" : "Invert Result",
          "description" : "If the check succeeds the score will be included in the total, for failure
 the score will not be incremented.",
          "propertyOrder" : 4200,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "geolocationDatabaseLocation" : {
```

```
          "title" : "Geolocation Database location",
          "description" : "The path to the location of the GEO location database.<br><br>The
 Geolocation database is not distributed with OpenAM, you can get it in binary format from <a href=
\"http://www.maxmind.com/app/country\" target=\"_blank\">MaxMind</a>.",
          "propertyOrder" : 3900,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "general" : {
      "type" : "object",
      "title" : "General",
      "propertyOrder" : 0,
      "properties" : {
        "authenticationLevel" : {
          "title" : "Authentication Level",
          "description" : "The authentication level associated with this module.<br><br>Each
 authentication module has an authentication level that can be used to indicate the level of security
 associated with the module; 0 is the lowest (and the default).",
          "propertyOrder" : 100,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "riskThreshold" : {
          "title" : "Risk Threshold",
          "description" : "If the risk threshold value is not reached after executing the different
 tests, the authentication is considered to be successful.<br><br>Associated with many of the adaptive
 risk checks is a score; if a check does not passes then the score is added to the current running
 total. The final score is then compared with the <i>Risk Threshold</i>, if the score is lesser than
 said threshold the module will be successful. ",
          "propertyOrder" : 200,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        }
      }
    },
    "authfailed" : {
      "type" : "object",
      "title" : "Failed Authentications",
      "propertyOrder" : 1,
      "properties" : {
        "failureScore" : {
          "title" : "Score",
          "description" : "The amount to increment the score if this check fails.",
          "propertyOrder" : 400,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "invertFailureScore" : {
          "title" : "Invert Result",
          "description" : "If the check succeeds the score will be included in the total, for failure
 the score will not be incremented.",
          "propertyOrder" : 500,
          "required" : true,
```

```
          "type" : "boolean",
          "exampleValue" : ""
        },
        "failedAuthenticationCheckEnabled" : {
          "title" : "Failed Authentication Check",
          "description" : "Checks if the user has past authentication failures.<br><br>Check if the
 OpenAM account lockout mechanism has recorded past authentication failures for the user.<br/><br/
><i>NB </i>For this check to function, Account Lockout must be enabled.",
          "propertyOrder" : 300,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        }
      }
    }
  }
}
```

Global Operations

Resource path: `/global-config/authentication/modules/adaptiverisk`

Resource version: `1.0`

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action AdaptiveRiskModule --global --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action AdaptiveRiskModule --global --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action AdaptiveRiskModule --global --actionName nextdescendents
```

read

Usage:

```
am> read AdaptiveRiskModule --global
```

update

Usage:

```
am> update AdaptiveRiskModule --global --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "defaults" : {
      "properties" : {
        "geolocation" : {
          "type" : "object",
          "title" : "Geo Location",
          "propertyOrder" : 8,
          "properties" : {
            "geolocationDatabaseLocation" : {
              "title" : "Geolocation Database location",
              "description" : "The path to the location of the GEO location database.<br><br>The
 Geolocation database is not distributed with OpenAM, you can get it in binary format from <a href=
\"http://www.maxmind.com/app/country\" target=\"_blank\">MaxMind</a>.",
              "propertyOrder" : 3900,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            },
            "geolocationValidCountryCodes" : {
              "title" : "Valid Country Codes",
              "description" : "The list of country codes that are considered as valid locations for
 client IPs.<br><br>The list is made up of country codes separated by a | character; for example:<br/
><br/><code>gb|us|no|fr</code>",
              "propertyOrder" : 4000,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            },
            "geolocationCheckEnabled" : {
              "title" : "Geolocation Country Code Check",
              "description" : "Enables the checking of the client IP address against the geolocation
 database.<br><br>The geolocation database associates IP addresses against their known location. This
 check passes if the country associated with the client IP address is matched against the list of
 valid country codes.<br/><br/>The geolocation database is available in binary format at <a href=
\"http://www.maxmind.com/app/country\" target=\"_blank\">MaxMind</a>.",
              "propertyOrder" : 3800,
              "required" : true,
              "type" : "boolean",
              "exampleValue" : ""
```

```
            },
            "geolocationScore" : {
              "title" : "Score",
              "description" : "The amount to increment the score if this check fails.",
              "propertyOrder" : 4100,
              "required" : true,
              "type" : "integer",
              "exampleValue" : ""
            },
            "invertGeolocationScore" : {
              "title" : "Invert Result",
              "description" : "If the check succeeds the score will be included in the total, for
failure the score will not be incremented.",
              "propertyOrder" : 4200,
              "required" : true,
              "type" : "boolean",
              "exampleValue" : ""
            }
          }
        },
        "devicecookie" : {
          "type" : "object",
          "title" : "Device Cookie",
          "propertyOrder" : 5,
          "properties" : {
            "invertDeviceCookieScore" : {
              "title" : "Invert Result",
              "description" : "If the check succeeds the score will be included in the total, for
failure the score will not be incremented.",
              "propertyOrder" : 3700,
              "required" : true,
              "type" : "boolean",
              "exampleValue" : ""
            },
            "deviceCookieScore" : {
              "title" : "Score",
              "description" : "The amount to increment the score if this check fails.",
              "propertyOrder" : 3600,
              "required" : true,
              "type" : "integer",
              "exampleValue" : ""
            },
            "deviceCookieCheckEnabled" : {
              "title" : "Device Registration Cookie Check",
              "description" : "Enables the checking of the client request for a known
cookie.<br><br>If this check is enabled, the check will pass if the client request contains the named
cookie.",
              "propertyOrder" : 3300,
              "required" : true,
              "type" : "boolean",
              "exampleValue" : ""
            },
            "saveDeviceCookieValueOnSuccessfulLogin" : {
              "title" : "Save Device Registration on Successful Login",
              "description" : "Set the device cookie on the client response<br><br>The Adaptive Risk
Post Authentication Plug-in will set the device cookie on the client response",
              "propertyOrder" : 3500,
              "required" : true,
              "type" : "boolean",
```

```
              "exampleValue" : ""
            },
            "deviceCookieName" : {
              "title" : "Cookie Name",
              "description" : "The name of the cookie to be checked for (and optionally set) on the
client request",
              "propertyOrder" : 3400,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            }
          }
        },
        "general" : {
          "type" : "object",
          "title" : "General",
          "propertyOrder" : 0,
          "properties" : {
            "authenticationLevel" : {
              "title" : "Authentication Level",
              "description" : "The authentication level associated with this module.<br><br>Each
authentication module has an authentication level that can be used to indicate the level of security
associated with the module; 0 is the lowest (and the default).",
              "propertyOrder" : 100,
              "required" : true,
              "type" : "integer",
              "exampleValue" : ""
            },
            "riskThreshold" : {
              "title" : "Risk Threshold",
              "description" : "If the risk threshold value is not reached after executing the
different tests, the authentication is considered to be successful.<br><br>Associated with many
of the adaptive risk checks is a score; if a check does not passes then the score is added to the
current running total. The final score is then compared with the <i>Risk Threshold</i>, if the score
is lesser than said threshold the module will be successful. ",
              "propertyOrder" : 200,
              "required" : true,
              "type" : "integer",
              "exampleValue" : ""
            }
          }
        },
        "iphistory" : {
          "type" : "object",
          "title" : "IP Address History",
          "propertyOrder" : 3,
          "properties" : {
            "ipHistoryScore" : {
              "title" : "Score",
              "description" : "The amount to increment the score if this check fails.",
              "propertyOrder" : 1400,
              "required" : true,
              "type" : "integer",
              "exampleValue" : ""
            },
            "ipHistoryCount" : {
              "title" : "History size",
              "description" : "The number of client IP addresses to save in the history list.",
              "propertyOrder" : 1100,
```

```
              "required" : true,
              "type" : "integer",
              "exampleValue" : ""
            },
            "saveSuccessfulIP" : {
              "title" : "Save Successful IP Address",
              "description" : "The IP History list will be updated in the data store<br><br>The
Adaptive Risk Post Authentication Plug-in will update the IP history list if the overall
authentication is successful.",
              "propertyOrder" : 1300,
              "required" : true,
              "type" : "boolean",
              "exampleValue" : ""
            },
            "invertIPHistoryScore" : {
              "title" : "Invert Result",
              "description" : "If the check succeeds the score will be included in the total, for
failure the score will not be incremented.",
              "propertyOrder" : 1500,
              "required" : true,
              "type" : "boolean",
              "exampleValue" : ""
            },
            "ipHistoryProfileAttribute" : {
              "title" : "Profile Attribute Name",
              "description" : "The name of the attribute used to store the IP history list in the data
store.<br><br>IP history list is stored in the Data Store meaning your Data Store should be able
to store values under the configured attribute name. If you're using a directory server as backend,
make sure your Data Store configuration contains the necessary objectclass and attribute related
settings.",
              "propertyOrder" : 1200,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            },
            "ipHistoryCheckEnabled" : {
              "title" : "IP History Check",
              "description" : "Enables the checking of client IP address against a list of past IP
addresses.<br><br>If this check is enabled; a set number of past IP addresses used by the client to
access OpenAM is recorded in the user profile. This check passes if the current client IP address
is present in the history list. If the IP address is not present, the check fails and the IP address
is added to list if the overall authentication is successful (causing the oldest IP address to be
removed).",
              "propertyOrder" : 1000,
              "required" : true,
              "type" : "boolean",
              "exampleValue" : ""
            }
          }
        },
        "lastlogin" : {
          "type" : "object",
          "title" : "Time Since Last Login",
          "propertyOrder" : 6,
          "properties" : {
            "saveLastLoginTimeOnSuccessfulLogin" : {
              "title" : "Save time of Successful Login",
              "description" : "The last login time will be saved in a client cookie<br><br>The
Adaptive Risk Post Authentication Plug-in will update the last login time",
```

```
              "propertyOrder" : 2500,
              "required" : true,
              "type" : "boolean",
              "exampleValue" : ""
            },
            "invertTimeSinceLastLoginScore" : {
              "title" : "Invert Result",
              "description" : "If the check succeeds the score will be included in the total, for
failure the score will not be incremented.",
              "propertyOrder" : 2700,
              "required" : true,
              "type" : "boolean",
              "exampleValue" : ""
            },
            "timeSinceLastLoginScore" : {
              "title" : "Score",
              "description" : "The amount to increment the score if this check fails.",
              "propertyOrder" : 2600,
              "required" : true,
              "type" : "integer",
              "exampleValue" : ""
            },
            "timeSinceLastLoginCookieName" : {
              "title" : "Cookie Name",
              "description" : "The name of the cookie used to store the time of the last successful
authentication.",
              "propertyOrder" : 2300,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            },
            "timeSinceLastLoginCheckEnabled" : {
              "title" : "Time since Last login Check",
              "description" : "Enables the checking of the last time the user successfully
authenticated.<br><br>If this check is enabled, the check ensures the user has successfully
authenticated within a given interval. If the interval has been exceeded the check will fail. The
last authentication for the user is stored in a client cookie.",
              "propertyOrder" : 2200,
              "required" : true,
              "type" : "boolean",
              "exampleValue" : ""
            },
            "maxTimeSinceLastLogin" : {
              "title" : "Max Time since Last login",
              "description" : "The maximum number of days that can elapse before this test.",
              "propertyOrder" : 2400,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            }
          }
        },
        "attributecheck" : {
          "type" : "object",
          "title" : "Profile Attribute",
          "propertyOrder" : 7,
          "properties" : {
            "profileRiskAttributeValue" : {
              "title" : "Attribute Value",
```

```
              "description" : "The required value of the named attribute.",
              "propertyOrder" : 3000,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            },
            "profileRiskAttributeName" : {
              "title" : "Attribute Name",
              "description" : "The name of the attribute to retrieve from the user profile in the data
store.",
              "propertyOrder" : 2900,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            },
            "profileRiskAttributeCheckEnabled" : {
              "title" : "Profile Risk Attribute check",
              "description" : "Enables the checking of the user profile for a matching attribute
and value.<br><br>If this check is enabled, the check will pass if the users profile contains the
required risk attribute and value.",
              "propertyOrder" : 2800,
              "required" : true,
              "type" : "boolean",
              "exampleValue" : ""
            },
            "invertProfileRiskAttributeScore" : {
              "title" : "Invert Result",
              "description" : "If the check succeeds the score will be included in the total, for
failure the score will not be incremented.",
              "propertyOrder" : 3200,
              "required" : true,
              "type" : "boolean",
              "exampleValue" : ""
            },
            "profileRiskAttributeScore" : {
              "title" : "Score",
              "description" : "The amount to increment the score if this check fails.",
              "propertyOrder" : 3100,
              "required" : true,
              "type" : "integer",
              "exampleValue" : ""
            }
          }
        },
        "iprange" : {
          "type" : "object",
          "title" : "IP Address Range",
          "propertyOrder" : 2,
          "properties" : {
            "ipRangeScore" : {
              "title" : "Score",
              "description" : "The amount to increment the score if this check fails.",
              "propertyOrder" : 800,
              "required" : true,
              "type" : "integer",
              "exampleValue" : ""
            },
            "ipRange" : {
              "title" : "IP Range",
```

```
              "description" : "The list of IP address to compare against the client IP
address.<br><br>The format of the IP address is as follows:<br/><br/><ul><li>Single IP address:
<code>172.16.90.1</code></li><li>CIDR notation: <code>172.16.90.0/24</code></li><li>IP net-block with
netmask: <code>172.16.90.0:255.255.255.0</code></li></ul>",
              "propertyOrder" : 700,
              "required" : true,
              "items" : {
                "type" : "string"
              },
              "type" : "array",
              "exampleValue" : ""
            },
            "ipRangeCheckEnabled" : {
              "title" : "IP Range Check",
              "description" : "Enables the checking of the client IP address against a list of IP
addresses.<br><br>The IP range check compares the IP of the client against a list of IP addresses, if
the client IP is found within said list the check is successful.",
              "propertyOrder" : 600,
              "required" : true,
              "type" : "boolean",
              "exampleValue" : ""
            },
            "invertIPRangeScoreEnabled" : {
              "title" : "Invert Result",
              "description" : "If the check succeeds the score will be included in the total, for
failure the score will not be incremented.",
              "propertyOrder" : 900,
              "required" : true,
              "type" : "boolean",
              "exampleValue" : ""
            }
          }
        },
        "knowncookie" : {
          "type" : "object",
          "title" : "Known Cookie",
          "propertyOrder" : 4,
          "properties" : {
            "createKnownCookieOnSuccessfulLogin" : {
              "title" : "Save Cookie Value on Successful Login",
              "description" : "The cookie will be created on the client after successful
login<br><br>The Adaptive Risk Post Authentication Plug-in will set the cookie on the client
response",
              "propertyOrder" : 1900,
              "required" : true,
              "type" : "boolean",
              "exampleValue" : ""
            },
            "knownCookieCheckEnabled" : {
              "title" : "Cookie Value Check",
              "description" : "Enables the checking of a known cookie value in the client
request<br><br>If this check is enabled, the check looks for a known cookie in the client request. If
the cookie exists and has the correct value then the check will pass. ",
              "propertyOrder" : 1600,
              "required" : true,
              "type" : "boolean",
              "exampleValue" : ""
            },
            "knownCookieName" : {
```

```
              "title" : "Cookie Name",
              "description" : "The name of the cookie to set on the client.",
              "propertyOrder" : 1700,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            },
            "invertKnownCookieScore" : {
              "title" : "Invert Result",
              "description" : "If the check succeeds the score will be included in the total, for
failure the score will not be incremented.",
              "propertyOrder" : 2100,
              "required" : true,
              "type" : "boolean",
              "exampleValue" : ""
            },
            "knownCookieScore" : {
              "title" : "Score",
              "description" : "The amount to increment the score if this check fails.",
              "propertyOrder" : 2000,
              "required" : true,
              "type" : "integer",
              "exampleValue" : ""
            },
            "knownCookieValue" : {
              "title" : "Cookie Value",
              "description" : "The value to be set on the cookie.",
              "propertyOrder" : 1800,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            }
          }
        },
        "requestheader" : {
          "type" : "object",
          "title" : "Request Header",
          "propertyOrder" : 9,
          "properties" : {
            "invertRequestHeaderScore" : {
              "title" : "Invert Result",
              "description" : "If the check succeeds the score will be included in the total, for
failure the score will not be incremented.",
              "propertyOrder" : 4700,
              "required" : true,
              "type" : "boolean",
              "exampleValue" : ""
            },
            "requestHeaderName" : {
              "title" : "Request Header Name",
              "description" : "The name of the required HTTP header ",
              "propertyOrder" : 4400,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            },
            "requestHeaderValue" : {
              "title" : "Request Header Value",
              "description" : "The required value of the named HTTP header.",
```

```
              "propertyOrder" : 4500,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            },
            "requestHeaderScore" : {
              "title" : "Score",
              "description" : "The amount to increment the score if this check fails.",
              "propertyOrder" : 4600,
              "required" : true,
              "type" : "integer",
              "exampleValue" : ""
            },
            "requestHeaderCheckEnabled" : {
              "title" : "Request Header Check",
              "description" : "Enables the checking of the client request for a known header name and
 value.<br><br>The request header check will pass if the client request contains the required named
 header and value.",
              "propertyOrder" : 4300,
              "required" : true,
              "type" : "boolean",
              "exampleValue" : ""
            }
          }
        },
        "authfailed" : {
          "type" : "object",
          "title" : "Failed Authentications",
          "propertyOrder" : 1,
          "properties" : {
            "invertFailureScore" : {
              "title" : "Invert Result",
              "description" : "If the check succeeds the score will be included in the total, for
 failure the score will not be incremented.",
              "propertyOrder" : 500,
              "required" : true,
              "type" : "boolean",
              "exampleValue" : ""
            },
            "failedAuthenticationCheckEnabled" : {
              "title" : "Failed Authentication Check",
              "description" : "Checks if the user has past authentication failures.<br><br>Check if
 the OpenAM account lockout mechanism has recorded past authentication failures for the user.<br/><br/
><i>NB </i>For this check to function, Account Lockout must be enabled.",
              "propertyOrder" : 300,
              "required" : true,
              "type" : "boolean",
              "exampleValue" : ""
            },
            "failureScore" : {
              "title" : "Score",
              "description" : "The amount to increment the score if this check fails.",
              "propertyOrder" : 400,
              "required" : true,
              "type" : "integer",
              "exampleValue" : ""
            }
          }
        }
```

```
      },
      "type" : "object",
      "title" : "Realm Defaults"
    }
  }
}
```

AdvancedProperties

Global Operations

An object of property key-value pairs

Resource path: `/global-config/servers/{serverName}/properties/advanced`

Resource version: `1.0`

read

Usage:

```
am> read AdvancedProperties --global --serverName serverName
```

Parameters:

`--serverName`

An object of property key-value pairs

update

Usage:

```
am> update AdvancedProperties --global --serverName serverName --body body
```

Parameters:

`--serverName`

An object of property key-value pairs

`--body`

The resource in JSON format, described by the following JSON schema:

```
{
  "patternProperties" : {
    ".+" : {
      "type" : "string",
      "title" : "Value",
      "description" : "Any string value"
    }
  },
  "$schema" : "http://json-schema.org/draft-04/schema#",
  "description" : "An object of property key-value pairs",
  "type" : "object",
  "title" : "Advanced Properties"
}
```

AgentDataStoreDecision

Realm Operations

Resource path: `/realm-config/authentication/authenticationtrees/nodes/AgentDataStoreDecisionNode`

Resource version: `1.0`

create

Usage:

```
am> create AgentDataStoreDecision --realm Realm --id id --body body
```

Parameters:

`--id`

The unique identifier for the resource.

`--body`

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "required" : [ ]
}
```

delete

Usage:

```
am> delete AgentDataStoreDecision --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action AgentDataStoreDecision --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action AgentDataStoreDecision --realm Realm --actionName getCreatableTypes
```

listOutcomes

List the available outcomes for the node type.

Usage:

```
am> action AgentDataStoreDecision --realm Realm --body body --actionName listOutcomes
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "title" : "Some configuration of the node. This does not need to be complete against the
 configuration schema."
}
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action AgentDataStoreDecision --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query AgentDataStoreDecision --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read AgentDataStoreDecision --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update AgentDataStoreDecision --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "required" : [ ]
}
```

AgentGroups

Realm Operations

Aggregating Agent Groups handler that is responsible for querying the aggregating agent groups

Resource path: `/realm-config/agents/groups`

Resource version: `1.0`

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action AgentGroups --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action AgentGroups --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action AgentGroups --realm Realm --actionName nextdescendents
```

query

Querying the aggregating agent groups

Usage:

```
am> query AgentGroups --realm Realm --filter filter
```

Parameters:

`--filter`

A CREST formatted query filter, where "true" will query all. Fields that can be queried: [*]

AgentService

Global Operations

Resource path: `/global-config/agents/AgentService`

Resource version: `1.0`

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action AgentService --global --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action AgentService --global --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action AgentService --global --actionName nextdescendents
```

read

Usage:

```
am> read AgentService --global
```

update

Usage:

```
am> update AgentService --global --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object"
}
```

Agents

Realm Operations

Aggregating Agents handler that is responsible for querying the aggregating agents

Resource path: `/realm-config/agents`

Resource version: `1.0`

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action Agents --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action Agents --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action Agents --realm Realm --actionName nextdescendents
```

query

Querying the aggregating agents

Usage:

```
am> query Agents --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all. Fields that can be queried: [*]

Global Operations

Global and default configuration for agents

Resource path: `/global-config/agents`

Resource version: `1.0`

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action Agents --global --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action Agents --global --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action Agents --global --actionName nextdescendents
```

AmsterModule

Realm Operations

Resource path: `/realm-config/authentication/modules/amster`

Resource version: `1.0`

create

Usage:

```
am> create AmsterModule --realm Realm --id id --body body
```

Parameters:

`--id`

The unique identifier for the resource.

`--body`

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "authorizedKeys" : {
      "title" : "Authorized Keys",
      "description" : "The location of the authorized_keys file (which has the same format as an
 OpenSSH authorized_keys file) to use to validate remote Amster connections.",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "enabled" : {
      "title" : "Enabled",
      "description" : "If not enabled, prevents PKI login using the Amster module.",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "authenticationLevel" : {
      "title" : "Authentication Level",
      "description" : "",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    }
  }
}
```

delete

Usage:

```
am> delete AmsterModule --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action AmsterModule --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action AmsterModule --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action AmsterModule --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query AmsterModule --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read AmsterModule --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update AmsterModule --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "authorizedKeys" : {
      "title" : "Authorized Keys",
      "description" : "The location of the authorized_keys file (which has the same format as an
 OpenSSH authorized_keys file) to use to validate remote Amster connections.",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "enabled" : {
      "title" : "Enabled",
      "description" : "If not enabled, prevents PKI login using the Amster module.",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "authenticationLevel" : {
      "title" : "Authentication Level",
      "description" : "",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    }
  }
}
```

Global Operations

Resource path: `/global-config/authentication/modules/amster`

Resource version: `1.0`

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action AmsterModule --global --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action AmsterModule --global --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action AmsterModule --global --actionName nextdescendents
```

read

Usage:

```
am> read AmsterModule --global
```

update

Usage:

```
am> update AmsterModule --global --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "defaults" : {
      "properties" : {
        "enabled" : {
          "title" : "Enabled",
          "description" : "If not enabled, prevents PKI login using the Amster module.",
          "propertyOrder" : 200,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "authenticationLevel" : {
          "title" : "Authentication Level",
          "description" : "",
          "propertyOrder" : 300,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "authorizedKeys" : {
          "title" : "Authorized Keys",
          "description" : "The location of the authorized_keys file (which has the same format as an
 OpenSSH authorized_keys file) to use to validate remote Amster connections.",
          "propertyOrder" : 100,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      },
      "type" : "object",
      "title" : "Realm Defaults"
    }
  }
}
```

AnonymousModule

Realm Operations

Resource path: `/realm-config/authentication/modules/anonymous`

Resource version: `1.0`

create

Usage:

```
am> create AnonymousModule --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "defaultAnonymousUsername" : {
      "title" : "Default Anonymous User Name",
      "description" : "The default username to use if no username is supplied during authentication.",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "caseSensitiveUsernameMatchingEnabled" : {
      "title" : "Case Sensitive User IDs",
      "description" : "If enabled, username matching will be case sensitive.",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "validAnonymousUsers" : {
      "title" : "Valid Anonymous Users",
      "description" : "List of accounts that are allowed to login without providing
 credentials.<br><br>Any username on this list will be allows anonymous access to OpenAM. Usernames
 listed here must have matching profiles in the data store or the user profile requirement must be
 disabled. The username can be specified during anonymous authentication as follows:<br/><br/><code>/
openam/UI/Login?module=anonymous&IDToken1=<i>username</i></code>",
      "propertyOrder" : 100,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "authenticationLevel" : {
      "title" : "Authentication Level",
      "description" : "The authentication level associated with this module.<br><br>Each
 authentication module has an authentication level that can be used to indicate the level of security
 associated with the module; 0 is the lowest (and the default).",
      "propertyOrder" : 400,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
```

```
    }
  }
}
```

delete

Usage:

```
am> delete AnonymousModule --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action AnonymousModule --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action AnonymousModule --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action AnonymousModule --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query AnonymousModule --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read AnonymousModule --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update AnonymousModule --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "defaultAnonymousUsername" : {
      "title" : "Default Anonymous User Name",
      "description" : "The default username to use if no username is supplied during authentication.",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "caseSensitiveUsernameMatchingEnabled" : {
```

```
      "title" : "Case Sensitive User IDs",
      "description" : "If enabled, username matching will be case sensitive.",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "validAnonymousUsers" : {
      "title" : "Valid Anonymous Users",
      "description" : "List of accounts that are allowed to login without providing
 credentials.<br><br>Any username on this list will be allows anonymous access to OpenAM. Usernames
 listed here must have matching profiles in the data store or the user profile requirement must be
 disabled. The username can be specified during anonymous authentication as follows:<br/><br/><code>/
openam/UI/Login?module=anonymous&IDToken1=<i>username</i></code>",
      "propertyOrder" : 100,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "authenticationLevel" : {
      "title" : "Authentication Level",
      "description" : "The authentication level associated with this module.<br><br>Each
 authentication module has an authentication level that can be used to indicate the level of security
 associated with the module; 0 is the lowest (and the default).",
      "propertyOrder" : 400,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    }
  }
}
```

Global Operations

Resource path: `/global-config/authentication/modules/anonymous`

Resource version: `1.0`

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action AnonymousModule --global --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action AnonymousModule --global --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action AnonymousModule --global --actionName nextdescendents
```

read

Usage:

```
am> read AnonymousModule --global
```

update

Usage:

```
am> update AnonymousModule --global --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "defaults" : {
      "properties" : {
        "validAnonymousUsers" : {
          "title" : "Valid Anonymous Users",
          "description" : "List of accounts that are allowed to login without providing
 credentials.<br><br>Any username on this list will be allows anonymous access to OpenAM. Usernames
 listed here must have matching profiles in the data store or the user profile requirement must be
 disabled. The username can be specified during anonymous authentication as follows:<br/><br/><code>/
openam/UI/Login?module=anonymous&IDToken1=<i>username</i></code>",
          "propertyOrder" : 100,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
```

```
        "defaultAnonymousUsername" : {
          "title" : "Default Anonymous User Name",
          "description" : "The default username to use if no username is supplied during
 authentication.",
          "propertyOrder" : 200,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "authenticationLevel" : {
          "title" : "Authentication Level",
          "description" : "The authentication level associated with this module.<br><br>Each
 authentication module has an authentication level that can be used to indicate the level of security
 associated with the module; 0 is the lowest (and the default).",
          "propertyOrder" : 400,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "caseSensitiveUsernameMatchingEnabled" : {
          "title" : "Case Sensitive User IDs",
          "description" : "If enabled, username matching will be case sensitive.",
          "propertyOrder" : 300,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        }
      },
      "type" : "object",
      "title" : "Realm Defaults"
    }
  }
}
```

AnonymousSessionUpgrade

Realm Operations

Resource path: `/realm-config/authentication/authenticationtrees/nodes/AnonymousSessionUpgradeNode`

Resource version: `1.0`

create

Usage:

```
am> create AnonymousSessionUpgrade --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "required" : [ ]
}
```

delete

Usage:

```
am> delete AnonymousSessionUpgrade --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action AnonymousSessionUpgrade --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action AnonymousSessionUpgrade --realm Realm --actionName getCreatableTypes
```

listOutcomes

List the available outcomes for the node type.

Usage:

```
am> action AnonymousSessionUpgrade --realm Realm --body body --actionName listOutcomes
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "title" : "Some configuration of the node. This does not need to be complete against the
 configuration schema."
}
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action AnonymousSessionUpgrade --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query AnonymousSessionUpgrade --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read AnonymousSessionUpgrade --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update AnonymousSessionUpgrade --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "required" : [ ]
}
```

AnonymousUserMapping

Realm Operations

Resource path: `/realm-config/authentication/authenticationtrees/nodes/AnonymousUserNode`

Resource version: `1.0`

create

Usage:

```
am> create AnonymousUserMapping --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "anonymousUserName" : {
      "title" : "Anonymous User Name",
      "description" : "The username of the user that will represent the anonymous user. This user
 account must already exist in the realm.",
      "propertyOrder" : 100,
      "type" : "string",
      "exampleValue" : ""
    }
  },
  "required" : [ "anonymousUserName" ]
}
```

delete

Usage:

```
am> delete AnonymousUserMapping --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action AnonymousUserMapping --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action AnonymousUserMapping --realm Realm --actionName getCreatableTypes
```

listOutcomes

List the available outcomes for the node type.

Usage:

```
am> action AnonymousUserMapping --realm Realm --body body --actionName listOutcomes
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "title" : "Some configuration of the node. This does not need to be complete against the
 configuration schema."
}
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action AnonymousUserMapping --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query AnonymousUserMapping --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read AnonymousUserMapping --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update AnonymousUserMapping --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "anonymousUserName" : {
      "title" : "Anonymous User Name",
      "description" : "The username of the user that will represent the anonymous user. This user
 account must already exist in the realm.",
      "propertyOrder" : 100,
      "type" : "string",
      "exampleValue" : ""
    }
  },
  "required" : [ "anonymousUserName" ]
}
```

ApplicationTypes

Realm Operations

Service for reading and listing the available application types. Application types act as templates for policy sets, and define how to compare resources and index policies. OpenAM provides a default application type that represents web resources called iPlanetAMWebAgentService

Resource path: `/applicationtypes`

Resource version: `1.0`

query

Lists the application types using a query filter

Usage:

```
am> query ApplicationTypes --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all. Fields that can be queried: [*]

read

Reads an individual application type by the provided application type name

Usage:

```
am> read ApplicationTypes --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

Applications

Realm Operations

Service for manipulating Applications. It supports the CRUDQ operations.

Resource path: `/applications`

Resource version: `2.1`

create

Creates a new Application in a realm

Usage:

```
am> create Applications --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "$schema" : "http://json-schema.org/draft-04/schema#",
  "description" : "Application schema",
  "type" : "object",
  "title" : "Application",
  "properties" : {
    "name" : {
      "type" : "string",
      "title" : "Name",
      "description" : "Unique application identifier."
    },
    "displayName" : {
      "type" : "string",
      "title" : "Display name",
      "description" : "When defined, it is displayed in the UI instead of application name."
    },
    "description" : {
      "type" : "string",
      "title" : "Description",
      "description" : "String describing the application."
    },
    "applicationType" : {
      "type" : "string",
      "title" : "Application type",
      "description" : "Name of the application type used as a template for the policy set."
    },
    "conditions" : {
      "type" : "array",
      "items" : {
        "type" : "string",
        "title" : "Conditions",
        "description" : "Condition types allowed in the context of the policy set."
      }
    },
    "subjects" : {
      "type" : "array",
      "items" : {
        "type" : "string",
        "title" : "Subjects",
        "description" : "Subject types allowed in the context of the policy set."
      }
    },
    "resourceTypeUuids" : {
      "type" : "array",
      "items" : {
        "type" : "string",
        "title" : "Resource type uuids",
        "description" : "A list of the UUIDs of the resource types associated with the policy set."
      }
    },
    "entitlementCombiner" : {
      "type" : "string",
      "title" : "Entitlement combiner",
      "description" : "Name of the decision combiner, such as \"DenyOverride\"."
    },
```

```
    "searchIndex" : {
      "type" : "string",
      "title" : "Search index",
      "description" : "Class name of the implementation for searching indexes for resource names, such
 as \"com.sun.identity.entitlement.util.ResourceNameSplitter\" for URL resource names."
    },
    "saveIndex" : {
      "type" : "string",
      "title" : "Save index",
      "description" : "Class name of the implementation for creating indexes for resource names, such
 as \"com.sun.identity.entitlement.util.ResourceNameIndexGenerator\" for URL resource names."
    },
    "resourceComparator" : {
      "type" : "string",
      "title" : "Resource comparator",
      "description" : "Class name of the resource comparator implementation
 used in the context of the policy set. The following implementations
 are available: \"com.sun.identity.entitlement.ExactMatchResourceName\",
 \"com.sun.identity.entitlement.PrefixResourceName\", \"com.sun.identity.entitlement.RegExResourceName
\", \"com.sun.identity.entitlement.URLResourceName\"."
    },
    "attributeNames" : {
      "type" : "array",
      "items" : {
        "type" : "string",
        "title" : "Attribute names",
        "description" : "A list of attribute names such as cn. The list is used to aid policy indexing
 and lookup."
      }
    },
    "createdBy" : {
      "type" : "string",
      "title" : "Created by",
      "description" : "A string containing the universal identifier DN of the subject that created the
 application."
    },
    "lastModifiedBy" : {
      "type" : "string",
      "title" : "Last modified by",
      "description" : "A string containing the universal identifier DN of the subject that most
 recently updated the application. If the application has not been modified since it was created, this
 will be the same value as createdBy."
    },
    "creationDate" : {
      "type" : "integer",
      "title" : "Creation date",
      "description" : "An integer containing the creation date and time, in number of seconds since
 the Unix Epoch."
    },
    "lastModifiedDate" : {
      "type" : "integer",
      "title" : "Last modified date",
      "description" : "An integer containing the last modified date and time, in number of seconds
 since the Unix Epoch. If the application has not been modified since it was created, this will be the
 same value as creationDate."
    },
    "editable" : {
      "type" : "boolean",
      "title" : "Editable",
```

```
      "description" : "It indicates if application is editable."
    }
  },
  "required" : [ "name", "applicationType" ]
}
```

delete

Deletes an individual Application in a realm specified by its name

Usage:

```
am> delete Applications --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

query

Lists all the Applications in a realm

Usage:

```
am> query Applications --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all. Fields that can be queried: [*]

read

Reads an individual Application in a realm specified by its name

Usage:

```
am> read Applications --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Updates an individual Application in a realm specified by its name

Usage:

```
am> update Applications --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "$schema" : "http://json-schema.org/draft-04/schema#",
  "description" : "Application schema",
  "type" : "object",
  "title" : "Application",
  "properties" : {
    "name" : {
      "type" : "string",
      "title" : "Name",
      "description" : "Unique application identifier."
    },
    "displayName" : {
      "type" : "string",
      "title" : "Display name",
      "description" : "When defined, it is displayed in the UI instead of application name."
    },
    "description" : {
      "type" : "string",
      "title" : "Description",
      "description" : "String describing the application."
    },
    "applicationType" : {
      "type" : "string",
      "title" : "Application type",
      "description" : "Name of the application type used as a template for the policy set."
    },
    "conditions" : {
      "type" : "array",
      "items" : {
        "type" : "string",
        "title" : "Conditions",
        "description" : "Condition types allowed in the context of the policy set."
      }
    },
    "subjects" : {
      "type" : "array",
      "items" : {
        "type" : "string",
        "title" : "Subjects",
        "description" : "Subject types allowed in the context of the policy set."
      }
    },
    "resourceTypeUuids" : {
      "type" : "array",
      "items" : {
```

```
        "type" : "string",
        "title" : "Resource type uuids",
        "description" : "A list of the UUIDs of the resource types associated with the policy set."
      }
    },
    "entitlementCombiner" : {
      "type" : "string",
      "title" : "Entitlement combiner",
      "description" : "Name of the decision combiner, such as \"DenyOverride\"."
    },
    "searchIndex" : {
      "type" : "string",
      "title" : "Search index",
      "description" : "Class name of the implementation for searching indexes for resource names, such
 as \"com.sun.identity.entitlement.util.ResourceNameSplitter\" for URL resource names."
    },
    "saveIndex" : {
      "type" : "string",
      "title" : "Save index",
      "description" : "Class name of the implementation for creating indexes for resource names, such
 as \"com.sun.identity.entitlement.util.ResourceNameIndexGenerator\" for URL resource names."
    },
    "resourceComparator" : {
      "type" : "string",
      "title" : "Resource comparator",
      "description" : "Class name of the resource comparator implementation
 used in the context of the policy set. The following implementations
 are available: \"com.sun.identity.entitlement.ExactMatchResourceName\",
 \"com.sun.identity.entitlement.PrefixResourceName\", \"com.sun.identity.entitlement.RegExResourceName
\", \"com.sun.identity.entitlement.URLResourceName\"."
    },
    "attributeNames" : {
      "type" : "array",
      "items" : {
        "type" : "string",
        "title" : "Attribute names",
        "description" : "A list of attribute names such as cn. The list is used to aid policy indexing
 and lookup."
      }
    },
    "createdBy" : {
      "type" : "string",
      "title" : "Created by",
      "description" : "A string containing the universal identifier DN of the subject that created the
 application."
    },
    "lastModifiedBy" : {
      "type" : "string",
      "title" : "Last modified by",
      "description" : "A string containing the universal identifier DN of the subject that most
 recently updated the application. If the application has not been modified since it was created, this
 will be the same value as createdBy."
    },
    "creationDate" : {
      "type" : "integer",
      "title" : "Creation date",
      "description" : "An integer containing the creation date and time, in number of seconds since
 the Unix Epoch."
    },
```

```
    "lastModifiedDate" : {
      "type" : "integer",
      "title" : "Last modified date",
      "description" : "An integer containing the last modified date and time, in number of seconds
 since the Unix Epoch. If the application has not been modified since it was created, this will be the
 same value as creationDate."
    },
    "editable" : {
      "type" : "boolean",
      "title" : "Editable",
      "description" : "It indicates if application is editable."
    }
  },
  "required" : [ "name", "applicationType" ]
}
```

AttributeCollector

Realm Operations

Resource path: `/realm-config/authentication/authenticationtrees/nodes/AttributeCollectorNode`

Resource version: `1.0`

create

Usage:

```
am> create AttributeCollector --realm Realm --id id --body body
```

Parameters:

`--id`

The unique identifier for the resource.

`--body`

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "identityAttribute" : {
      "title" : "Identity Attribute",
      "description" : "The attribute used to identify the the object in IDM.",
      "propertyOrder" : 400,
      "type" : "string",
      "exampleValue" : ""
    },
```

```
    "required" : {
      "title" : "All Attributes Required",
      "description" : "When set, requires all attributes collected to contain non-null values.",
      "propertyOrder" : 200,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "validateInputs" : {
      "title" : "Validate Input",
      "description" : "Set to true if client input should be validated against IDM policy as declared
 in the schema.",
      "propertyOrder" : 300,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "attributesToCollect" : {
      "title" : "Attributes to Collect",
      "description" : "A set of attributes to collect from the client.",
      "propertyOrder" : 100,
      "items" : {
        "type" : "string"
      },
      "minItems" : 1,
      "type" : "array",
      "exampleValue" : ""
    }
  },
  "required" : [ "attributesToCollect", "validateInputs", "identityAttribute", "required" ]
}
```

delete

Usage:

```
am> delete AttributeCollector --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action AttributeCollector --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action AttributeCollector --realm Realm --actionName getCreatableTypes
```

listOutcomes

List the available outcomes for the node type.

Usage:

```
am> action AttributeCollector --realm Realm --body body --actionName listOutcomes
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "title" : "Some configuration of the node. This does not need to be complete against the
 configuration schema."
}
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action AttributeCollector --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query AttributeCollector --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read AttributeCollector --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update AttributeCollector --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "identityAttribute" : {
      "title" : "Identity Attribute",
      "description" : "The attribute used to identify the the object in IDM.",
      "propertyOrder" : 400,
      "type" : "string",
      "exampleValue" : ""
    },
    "required" : {
      "title" : "All Attributes Required",
      "description" : "When set, requires all attributes collected to contain non-null values.",
      "propertyOrder" : 200,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "validateInputs" : {
      "title" : "Validate Input",
      "description" : "Set to true if client input should be validated against IDM policy as declared
 in the schema.",
      "propertyOrder" : 300,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "attributesToCollect" : {
      "title" : "Attributes to Collect",
      "description" : "A set of attributes to collect from the client.",
      "propertyOrder" : 100,
      "items" : {
        "type" : "string"
      },
      "minItems" : 1,
      "type" : "array",
```

```
      "exampleValue" : ""
    }
  },
  "required" : [ "attributesToCollect", "validateInputs", "identityAttribute", "required" ]
}
```

AttributePresentDecision

Realm Operations

Resource path: `/realm-config/authentication/authenticationtrees/nodes/AttributePresentDecisionNode`

Resource version: `1.0`

create

Usage:

```
am> create AttributePresentDecision --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "identityAttribute" : {
      "title" : "Identity Attribute",
      "description" : "The attribute to query in the IDM object.",
      "propertyOrder" : 200,
      "type" : "string",
      "exampleValue" : ""
    },
    "presentAttribute" : {
      "title" : "Present Attribute",
      "description" : "The object attribute to verify is present regardless of whether the field is
 private.",
      "propertyOrder" : 100,
      "type" : "string",
      "exampleValue" : ""
    }
  },
  "required" : [ "presentAttribute", "identityAttribute" ]
}
```

delete

Usage:

```
am> delete AttributePresentDecision --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action AttributePresentDecision --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action AttributePresentDecision --realm Realm --actionName getCreatableTypes
```

listOutcomes

List the available outcomes for the node type.

Usage:

```
am> action AttributePresentDecision --realm Realm --body body --actionName listOutcomes
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "title" : "Some configuration of the node. This does not need to be complete against the
 configuration schema."
}
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action AttributePresentDecision --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query AttributePresentDecision --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read AttributePresentDecision --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update AttributePresentDecision --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "identityAttribute" : {
      "title" : "Identity Attribute",
      "description" : "The attribute to query in the IDM object.",
      "propertyOrder" : 200,
      "type" : "string",
      "exampleValue" : ""
    },
    "presentAttribute" : {
      "title" : "Present Attribute",
      "description" : "The object attribute to verify is present regardless of whether the field is
 private.",
      "propertyOrder" : 100,
      "type" : "string",
      "exampleValue" : ""
    }
  },
  "required" : [ "presentAttribute", "identityAttribute" ]
}
```

AttributeValueDecision

Realm Operations

Resource path: `/realm-config/authentication/authenticationtrees/nodes/AttributeValueDecisionNode`

Resource version: `1.0`

create

Usage:

```
am> create AttributeValueDecision --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
```

```
    "identityAttribute" : {
      "title" : "Identity Attribute",
      "description" : "The attribute to query in the IDM object.",
      "propertyOrder" : 400,
      "type" : "string",
      "exampleValue" : ""
    },
    "comparisonValue" : {
      "title" : "Comparison Value",
      "description" : "If using the EQUALS comparison operation, the value to compare the object's
 attribute value to.",
      "propertyOrder" : 300,
      "type" : "string",
      "exampleValue" : ""
    },
    "comparisonOperation" : {
      "title" : "Comparison Operation",
      "description" : "The operation to perform on the object attribute; PRESENT checks for existence
 of an attribute, EQUALS checks if the object's attribute value equals the configured comparison
 value.",
      "propertyOrder" : 200,
      "type" : "string",
      "exampleValue" : ""
    },
    "comparisonAttribute" : {
      "title" : "Comparison Attribute",
      "description" : "The object attribute to compare.",
      "propertyOrder" : 100,
      "type" : "string",
      "exampleValue" : ""
    }
  },
  "required" : [ "identityAttribute", "comparisonOperation", "comparisonAttribute" ]
}
```

delete

Usage:

```
am> delete AttributeValueDecision --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action AttributeValueDecision --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action AttributeValueDecision --realm Realm --actionName getCreatableTypes
```

listOutcomes

List the available outcomes for the node type.

Usage:

```
am> action AttributeValueDecision --realm Realm --body body --actionName listOutcomes
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "title" : "Some configuration of the node. This does not need to be complete against the
 configuration schema."
}
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action AttributeValueDecision --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query AttributeValueDecision --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read AttributeValueDecision --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update AttributeValueDecision --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "identityAttribute" : {
      "title" : "Identity Attribute",
      "description" : "The attribute to query in the IDM object.",
      "propertyOrder" : 400,
      "type" : "string",
      "exampleValue" : ""
    },
    "comparisonValue" : {
      "title" : "Comparison Value",
      "description" : "If using the EQUALS comparison operation, the value to compare the object's
 attribute value to.",
      "propertyOrder" : 300,
      "type" : "string",
      "exampleValue" : ""
    },
    "comparisonOperation" : {
      "title" : "Comparison Operation",
      "description" : "The operation to perform on the object attribute; PRESENT checks for existence
 of an attribute, EQUALS checks if the object's attribute value equals the configured comparison
 value.",
      "propertyOrder" : 200,
      "type" : "string",
      "exampleValue" : ""
    },
    "comparisonAttribute" : {
      "title" : "Comparison Attribute",
      "description" : "The object attribute to compare.",
```

```
      "propertyOrder" : 100,
      "type" : "string",
      "exampleValue" : ""
    }
  },
  "required" : [ "identityAttribute", "comparisonOperation", "comparisonAttribute" ]
}
```

AuditEvent

Realm Operations

Audit events are logged through a realm audit service.

Resource path: `/realm-audit/{topic}`

Resource version: `1.0`

create

Create a new audit event, which will be handled and logged by the configured audit service.

Usage:

```
am> create AuditEvent --realm Realm --topic topic --body body
```

Parameters:

--topic

Audit events are logged through a realm audit service.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "$schema" : "http://json-schema.org/draft-04/schema#",
  "description" : "The schema contains properties that are common to all topics and some that are
 unique to a specific topic. The description of each property indicates which topic the property
 applies to.",
  "title" : "Audit event schema",
  "type" : "object",
  "properties" : {
    "_id" : {
      "title" : "ID",
      "description" : "The ID of the event, used by all topics",
      "type" : "string"
    },
    "timestamp" : {
      "title" : "Timestamp",
      "description" : "The time at which the event occurred, used by all topics",
      "type" : "string"
```

```
    },
    "eventName" : {
      "title" : "Event name",
      "description" : "The name of the event, used by all topics",
      "type" : "string"
    },
    "transactionId" : {
      "title" : "Transaction ID",
      "description" : "The transaction ID of the event, used by all topics",
      "type" : "string"
    },
    "userId" : {
      "title" : "User ID",
      "description" : "The ID of the user responsible for the event, used by all topics",
      "type" : "string"
    },
    "trackingIds" : {
      "title" : "Tracking IDs",
      "description" : "The tracking IDs of the event, used by all topics",
      "type" : "array",
      "items" : {
        "id" : "0",
        "type" : "string"
      }
    },
    "component" : {
      "title" : "Component",
      "description" : "The component responsible for the event, used by all topics",
      "type" : "string"
    },
    "realm" : {
      "title" : "Realm",
      "description" : "The realm in which the event occurred, used by all topics",
      "type" : "string"
    },
    "server" : {
      "title" : "Server",
      "description" : "The server details for an access event",
      "type" : "object",
      "properties" : {
        "ip" : {
          "title" : "Server IP address",
          "description" : "The server ip address for an access event",
          "type" : "string"
        },
        "port" : {
          "title" : "Server port",
          "description" : "The server port for an access event",
          "type" : "integer"
        }
      }
    },
    "client" : {
      "title" : "Client",
      "description" : "The client details for an access event",
      "type" : "object",
      "properties" : {
        "ip" : {
          "title" : "Client IP address",
```

```
          "description" : "The client IP address for an access event",
          "type" : "string"
        },
        "port" : {
          "title" : "Client port",
          "description" : "The client port for an access event",
          "type" : "integer"
        }
      }
    },
    "request" : {
      "title" : "Request",
      "description" : "The request details for an access event",
      "type" : "object",
      "properties" : {
        "protocol" : {
          "title" : "Request protocol",
          "description" : "The request protocol for an access event",
          "type" : "string"
        },
        "operation" : {
          "title" : "Request operation",
          "description" : "The request operation for an access event",
          "type" : "string"
        },
        "detail" : {
          "title" : "Request detail",
          "description" : "The request detail for an access event",
          "type" : "object"
        }
      }
    },
    "http" : {
      "title" : "Http details",
      "description" : "The Http details for an access event",
      "type" : "object",
      "properties" : {
        "request" : {
          "title" : "Http request",
          "description" : "The http request for an access event",
          "type" : "object",
          "properties" : {
            "secure" : {
              "title" : "Http secure",
              "description" : "The http secure property for an access event",
              "type" : "boolean"
            },
            "method" : {
              "title" : "Http method",
              "description" : "The http method for an access event",
              "type" : "string"
            },
            "path" : {
              "title" : "Http path",
              "description" : "The http path for an access event",
              "type" : "string"
            },
            "queryParameters" : {
              "title" : "Http query parameters",
```

```
            "description" : "The http query parameters for an access event",
            "type" : "object",
            "additionalProperties" : {
              "type" : "array",
              "items" : {
                "type" : "string"
              }
            }
          },
          "headers" : {
            "title" : "Http headers",
            "description" : "The http headers for an access event",
            "type" : "object",
            "additionalProperties" : {
              "type" : "array",
              "items" : {
                "type" : "string"
              }
            }
          },
          "cookies" : {
            "title" : "Http cookies",
            "description" : "The http cookies for an access event",
            "type" : "object",
            "additionalProperties" : {
              "type" : "string"
            }
          }
        }
      },
      "response" : {
        "title" : "Http response",
        "description" : "The http response for an access event",
        "type" : "object",
        "properties" : {
          "headers" : {
            "title" : "Http request headers",
            "description" : "The http request headers for an access event",
            "type" : "object",
            "additionalProperties" : {
              "type" : "array",
              "items" : {
                "type" : "string"
              }
            }
          }
        }
      }
    }
  },
  "response" : {
    "title" : "Response",
    "description" : "The response details for an access event",
    "type" : "object",
    "properties" : {
      "status" : {
        "title" : "Response status",
        "description" : "The response status for an access event",
        "type" : "string"
```

```
        },
        "statusCode" : {
          "title" : "Response status code",
          "description" : "The response status code for an access event",
          "type" : "string"
        },
        "detail" : {
          "title" : "Response detail",
          "description" : "The response detail for an access event",
          "type" : "object"
        },
        "elapsedTime" : {
          "title" : "Response elapsed time",
          "description" : "The response elapsedTime for an access event",
          "type" : "integer"
        },
        "elapsedTimeUnits" : {
          "title" : "Response elapsed time units",
          "description" : "The response elapsed time units for an access event",
          "type" : "string"
        }
      }
    },
    "runAs" : {
      "title" : "Run as",
      "description" : "What the change that triggered an activity or config event was run as",
      "type" : "string"
    },
    "objectId" : {
      "title" : "Object ID",
      "description" : "The object ID of the change that triggered an activity or config event",
      "type" : "string"
    },
    "operation" : {
      "title" : "Operation",
      "description" : "The operation that triggered an activity or config event",
      "type" : "string"
    },
    "before" : {
      "title" : "Before state",
      "description" : "The state before an activity or config event occurred",
      "type" : "object"
    },
    "after" : {
      "title" : "After state",
      "description" : "The state after an activity or config event occurred",
      "type" : "object"
    },
    "changedFields" : {
      "title" : "Changed fields",
      "description" : "The changed fields after an activity or config event occurred",
      "type" : "array",
      "items" : {
        "id" : "1",
        "type" : "string"
      }
    },
    "revision" : {
      "title" : "Revision",
```

```
      "description" : "The revision for an activity or config event",
      "type" : "string"
    },
    "result" : {
      "title" : "Result",
      "description" : "The result of the authentication event",
      "type" : "string"
    },
    "principal" : {
      "title" : "Principal",
      "description" : "The principal responsible for the authentication event",
      "type" : "array",
      "items" : {
        "type" : "string"
      }
    },
    "context" : {
      "title" : "Context",
      "description" : "The context of an authentication event",
      "type" : "object",
      "properties" : { }
    },
    "entries" : {
      "title" : "Entries",
      "description" : "The entries for an authentication event",
      "type" : "array",
      "items" : {
        "type" : "object",
        "properties" : {
          "moduleId" : {
            "title" : "Module ID",
            "description" : "The module ID for the authentication event",
            "type" : "string"
          },
          "result" : {
            "title" : "Module result",
            "description" : "The result of the module authentication event",
            "type" : "string"
          },
          "info" : {
            "title" : "Entries information",
            "description" : "The entries information for an authentication event",
            "type" : "object",
            "properties" : { }
          }
        }
      }
    }
  },
  "required" : [ "transactionId", "timestamp" ]
}
```

Global Operations

Audit events are logged through the global audit service.

Resource path: `/global-audit/{topic}`

Resource version: `1.0`

create

Create a new audit event, which will be handled and logged by the configured audit service.

Usage:

```
am> create AuditEvent --global --topic topic --body body
```

Parameters:

--topic

Audit events are logged through the global audit service.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "$schema" : "http://json-schema.org/draft-04/schema#",
  "description" : "The schema contains properties that are common to all topics and some that are
 unique to a specific topic. The description of each property indicates which topic the property
 applies to.",
  "title" : "Audit event schema",
  "type" : "object",
  "properties" : {
    "_id" : {
      "title" : "ID",
      "description" : "The ID of the event, used by all topics",
      "type" : "string"
    },
    "timestamp" : {
      "title" : "Timestamp",
      "description" : "The time at which the event occurred, used by all topics",
      "type" : "string"
    },
    "eventName" : {
      "title" : "Event name",
      "description" : "The name of the event, used by all topics",
      "type" : "string"
    },
    "transactionId" : {
      "title" : "Transaction ID",
      "description" : "The transaction ID of the event, used by all topics",
      "type" : "string"
    },
    "userId" : {
      "title" : "User ID",
      "description" : "The ID of the user responsible for the event, used by all topics",
      "type" : "string"
    },
    "trackingIds" : {
      "title" : "Tracking IDs",
```

```
      "description" : "The tracking IDs of the event, used by all topics",
      "type" : "array",
      "items" : {
        "id" : "0",
        "type" : "string"
      }
    },
    "component" : {
      "title" : "Component",
      "description" : "The component responsible for the event, used by all topics",
      "type" : "string"
    },
    "realm" : {
      "title" : "Realm",
      "description" : "The realm in which the event occurred, used by all topics",
      "type" : "string"
    },
    "server" : {
      "title" : "Server",
      "description" : "The server details for an access event",
      "type" : "object",
      "properties" : {
        "ip" : {
          "title" : "Server IP address",
          "description" : "The server ip address for an access event",
          "type" : "string"
        },
        "port" : {
          "title" : "Server port",
          "description" : "The server port for an access event",
          "type" : "integer"
        }
      }
    },
    "client" : {
      "title" : "Client",
      "description" : "The client details for an access event",
      "type" : "object",
      "properties" : {
        "ip" : {
          "title" : "Client IP address",
          "description" : "The client IP address for an access event",
          "type" : "string"
        },
        "port" : {
          "title" : "Client port",
          "description" : "The client port for an access event",
          "type" : "integer"
        }
      }
    },
    "request" : {
      "title" : "Request",
      "description" : "The request details for an access event",
      "type" : "object",
      "properties" : {
        "protocol" : {
          "title" : "Request protocol",
          "description" : "The request protocol for an access event",
```

```
          "type" : "string"
        },
        "operation" : {
          "title" : "Request operation",
          "description" : "The request operation for an access event",
          "type" : "string"
        },
        "detail" : {
          "title" : "Request detail",
          "description" : "The request detail for an access event",
          "type" : "object"
        }
      }
    },
    "http" : {
      "title" : "Http details",
      "description" : "The Http details for an access event",
      "type" : "object",
      "properties" : {
        "request" : {
          "title" : "Http request",
          "description" : "The http request for an access event",
          "type" : "object",
          "properties" : {
            "secure" : {
              "title" : "Http secure",
              "description" : "The http secure property for an access event",
              "type" : "boolean"
            },
            "method" : {
              "title" : "Http method",
              "description" : "The http method for an access event",
              "type" : "string"
            },
            "path" : {
              "title" : "Http path",
              "description" : "The http path for an access event",
              "type" : "string"
            },
            "queryParameters" : {
              "title" : "Http query parameters",
              "description" : "The http query parameters for an access event",
              "type" : "object",
              "additionalProperties" : {
                "type" : "array",
                "items" : {
                  "type" : "string"
                }
              }
            },
            "headers" : {
              "title" : "Http headers",
              "description" : "The http headers for an access event",
              "type" : "object",
              "additionalProperties" : {
                "type" : "array",
                "items" : {
                  "type" : "string"
                }
```

```
            }
          },
          "cookies" : {
            "title" : "Http cookies",
            "description" : "The http cookies for an access event",
            "type" : "object",
            "additionalProperties" : {
              "type" : "string"
            }
          }
        }
      },
      "response" : {
        "title" : "Http response",
        "description" : "The http response for an access event",
        "type" : "object",
        "properties" : {
          "headers" : {
            "title" : "Http request headers",
            "description" : "The http request headers for an access event",
            "type" : "object",
            "additionalProperties" : {
              "type" : "array",
              "items" : {
                "type" : "string"
              }
            }
          }
        }
      }
    }
  },
  "response" : {
    "title" : "Response",
    "description" : "The response details for an access event",
    "type" : "object",
    "properties" : {
      "status" : {
        "title" : "Response status",
        "description" : "The response status for an access event",
        "type" : "string"
      },
      "statusCode" : {
        "title" : "Response status code",
        "description" : "The response status code for an access event",
        "type" : "string"
      },
      "detail" : {
        "title" : "Response detail",
        "description" : "The response detail for an access event",
        "type" : "object"
      },
      "elapsedTime" : {
        "title" : "Response elapsed time",
        "description" : "The response elapsedTime for an access event",
        "type" : "integer"
      },
      "elapsedTimeUnits" : {
        "title" : "Response elapsed time units",
```

```
        "description" : "The response elapsed time units for an access event",
        "type" : "string"
      }
    }
  },
  "runAs" : {
    "title" : "Run as",
    "description" : "What the change that triggered an activity or config event was run as",
    "type" : "string"
  },
  "objectId" : {
    "title" : "Object ID",
    "description" : "The object ID of the change that triggered an activity or config event",
    "type" : "string"
  },
  "operation" : {
    "title" : "Operation",
    "description" : "The operation that triggered an activity or config event",
    "type" : "string"
  },
  "before" : {
    "title" : "Before state",
    "description" : "The state before an activity or config event occurred",
    "type" : "object"
  },
  "after" : {
    "title" : "After state",
    "description" : "The state after an activity or config event occurred",
    "type" : "object"
  },
  "changedFields" : {
    "title" : "Changed fields",
    "description" : "The changed fields after an activity or config event occurred",
    "type" : "array",
    "items" : {
      "id" : "1",
      "type" : "string"
    }
  },
  "revision" : {
    "title" : "Revision",
    "description" : "The revision for an activity or config event",
    "type" : "string"
  },
  "result" : {
    "title" : "Result",
    "description" : "The result of the authentication event",
    "type" : "string"
  },
  "principal" : {
    "title" : "Principal",
    "description" : "The principal responsible for the authentication event",
    "type" : "array",
    "items" : {
      "type" : "string"
    }
  },
  "context" : {
    "title" : "Context",
```

```
      "description" : "The context of an authentication event",
      "type" : "object",
      "properties" : { }
    },
    "entries" : {
      "title" : "Entries",
      "description" : "The entries for an authentication event",
      "type" : "array",
      "items" : {
        "type" : "object",
        "properties" : {
          "moduleId" : {
            "title" : "Module ID",
            "description" : "The module ID for the authentication event",
            "type" : "string"
          },
          "result" : {
            "title" : "Module result",
            "description" : "The result of the module authentication event",
            "type" : "string"
          },
          "info" : {
            "title" : "Entries information",
            "description" : "The entries information for an authentication event",
            "type" : "object",
            "properties" : { }
          }
        }
      }
    }
  },
  "required" : [ "transactionId", "timestamp" ]
}
```

AuditLogging

Realm Operations

Resource path: `/realm-config/services/audit`

Resource version: `1.0`

create

Usage:

```
am> create AuditLogging --realm Realm --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "blacklistFieldFilters" : {
      "title" : "Field blacklist filters",
      "description" : "Blacklist filters can be used to remove audit event fields which are
 whitelisted by default. These are fields which are safe to log but which you have decided are not
 necessary for your requirements. <p> Each field filter should be provided using a JSON Pointer-
like syntax which is prefixed with the event's topic. The topic will be one of <code>access</code>,
 <code>activity</code>, <code>authentication</code>, or <code>config</code>.<p> For example, you might
 want to filter out surnames by hiding the <code>sn</code> field from <em>activity</em> events. To do
 so, add the following pointers to the Field blacklist filters list: <ul><li><code>/activity/before/
sn</code></li><li><code>/activity/after/sn</code></li></ul>",
      "propertyOrder" : 300,
      "required" : false,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "auditEnabled" : {
      "title" : "Audit logging",
      "description" : "Enable audit logging in OpenAM.",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "whitelistFieldFilters" : {
      "title" : "Field whitelist filters",
      "description" : "OpenAM has a predefined whitelist built-in that only records values that
 do not contain sensitive information. Use this property to whitelist fields in addition to the
 built-in list. <p> Each field filter should be provided using a JSON Pointer-like syntax which is
 prefixed with the event's topic. The topic will be one of <code>access</code>, <code>activity</code>,
 <code>authentication</code>, or <code>config</code>.<p> For example, to record the values of the
 <code>Accept-Language</code> HTTP header in <em>access</em> events, the pointer is <code>/access/
http/request/headers/accept-language</code>.",
      "propertyOrder" : 200,
      "required" : false,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    }
  }
}
```

delete

Usage:

```
am> delete AuditLogging --realm Realm
```

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action AuditLogging --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action AuditLogging --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action AuditLogging --realm Realm --actionName nextdescendents
```

read

Usage:

```
am> read AuditLogging --realm Realm
```

update

Usage:

```
am> update AuditLogging --realm Realm --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "blacklistFieldFilters" : {
```

```
      "title" : "Field blacklist filters",
      "description" : "Blacklist filters can be used to remove audit event fields which are
 whitelisted by default. These are fields which are safe to log but which you have decided are not
 necessary for your requirements. <p> Each field filter should be provided using a JSON Pointer-
like syntax which is prefixed with the event's topic. The topic will be one of <code>access</code>,
 <code>activity</code>, <code>authentication</code>, or <code>config</code>.<p> For example, you might
 want to filter out surnames by hiding the <code>sn</code> field from <em>activity</em> events. To do
 so, add the following pointers to the Field blacklist filters list: <ul><li><code>/activity/before/
sn</code></li><li><code>/activity/after/sn</code></li></ul>",
      "propertyOrder" : 300,
      "required" : false,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "auditEnabled" : {
      "title" : "Audit logging",
      "description" : "Enable audit logging in OpenAM.",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "whitelistFieldFilters" : {
      "title" : "Field whitelist filters",
      "description" : "OpenAM has a predefined whitelist built-in that only records values that
 do not contain sensitive information. Use this property to whitelist fields in addition to the
 built-in list. <p> Each field filter should be provided using a JSON Pointer-like syntax which is
 prefixed with the event's topic. The topic will be one of <code>access</code>, <code>activity</code>,
 <code>authentication</code>, or <code>config</code>.<p> For example, to record the values of the
 <code>Accept-Language</code> HTTP header in <em>access</em> events, the pointer is <code>/access/
http/request/headers/accept-language</code>.",
      "propertyOrder" : 200,
      "required" : false,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    }
  }
}
```


Global Operations

Resource path: `/global-config/services/audit`

Resource version: `1.0`

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action AuditLogging --global --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action AuditLogging --global --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action AuditLogging --global --actionName nextdescendents
```

read

Usage:

```
am> read AuditLogging --global
```

update

Usage:

```
am> update AuditLogging --global --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "auditEnabled" : {
      "title" : "Audit logging",
      "description" : "Enable audit logging in OpenAM.",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "blacklistFieldFilters" : {
      "title" : "Field blacklist filters",
```

```
      "description" : "Blacklist filters can be used to remove audit event fields which are
 whitelisted by default. These are fields which are safe to log but which you have decided are not
 necessary for your requirements. <p> Each field filter should be provided using a JSON Pointer-
like syntax which is prefixed with the event's topic. The topic will be one of <code>access</code>,
 <code>activity</code>, <code>authentication</code>, or <code>config</code>.<p> For example, you might
 want to filter out surnames by hiding the <code>sn</code> field from <em>activity</em> events. To do
 so, add the following pointers to the Field blacklist filters list: <ul><li><code>/activity/before/
sn</code></li><li><code>/activity/after/sn</code></li></ul>",
      "propertyOrder" : 300,
      "required" : false,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "whitelistFieldFilters" : {
      "title" : "Field whitelist filters",
      "description" : "OpenAM has a predefined whitelist built-in that only records values that
 do not contain sensitive information. Use this property to whitelist fields in addition to the
 built-in list. <p> Each field filter should be provided using a JSON Pointer-like syntax which is
 prefixed with the event's topic. The topic will be one of <code>access</code>, <code>activity</code>,
 <code>authentication</code>, or <code>config</code>.<p> For example, to record the values of the
 <code>Accept-Language</code> HTTP header in <em>access</em> events, the pointer is <code>/access/
http/request/headers/accept-language</code>.",
      "propertyOrder" : 200,
      "required" : false,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "defaults" : {
      "properties" : {
        "whitelistFieldFilters" : {
          "title" : "Field whitelist filters",
          "description" : "OpenAM has a predefined whitelist built-in that only records values that
 do not contain sensitive information. Use this property to whitelist fields in addition to the
 built-in list. <p> Each field filter should be provided using a JSON Pointer-like syntax which is
 prefixed with the event's topic. The topic will be one of <code>access</code>, <code>activity</code>,
 <code>authentication</code>, or <code>config</code>.<p> For example, to record the values of the
 <code>Accept-Language</code> HTTP header in <em>access</em> events, the pointer is <code>/access/
http/request/headers/accept-language</code>.",
          "propertyOrder" : 200,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "auditEnabled" : {
          "title" : "Audit logging",
          "description" : "Enable audit logging in OpenAM.",
          "propertyOrder" : 100,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
```

```
        },
        "blacklistFieldFilters" : {
          "title" : "Field blacklist filters",
          "description" : "Blacklist filters can be used to remove audit event fields which are
 whitelisted by default. These are fields which are safe to log but which you have decided are not
 necessary for your requirements. <p> Each field filter should be provided using a JSON Pointer-
like syntax which is prefixed with the event's topic. The topic will be one of <code>access</code>,
 <code>activity</code>, <code>authentication</code>, or <code>config</code>.<p> For example, you might
 want to filter out surnames by hiding the <code>sn</code> field from <em>activity</em> events. To do
 so, add the following pointers to the Field blacklist filters list: <ul><li><code>/activity/before/
sn</code></li><li><code>/activity/after/sn</code></li></ul>",
          "propertyOrder" : 300,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        }
      },
      "type" : "object",
      "title" : "Realm Defaults"
    }
  }
}
```

AuthLevelDecision

Realm Operations

Resource path: `/realm-config/authentication/authenticationtrees/nodes/AuthLevelDecisionNode`

Resource version: `1.0`

create

Usage:

```
am> create AuthLevelDecision --realm Realm --id id --body body
```

Parameters:

`--id`

The unique identifier for the resource.

`--body`

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "authLevelRequirement" : {
      "title" : "Sufficient Authentication Level",
      "description" : "The current authentication level must be greater than or equal to this value
 for the decision to return true.",
      "propertyOrder" : 100,
      "type" : "integer",
      "exampleValue" : ""
    }
  },
  "required" : [ "authLevelRequirement" ]
}
```

delete

Usage:

```
am> delete AuthLevelDecision --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action AuthLevelDecision --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action AuthLevelDecision --realm Realm --actionName getCreatableTypes
```

listOutcomes

List the available outcomes for the node type.

Usage:

```
am> action AuthLevelDecision --realm Realm --body body --actionName listOutcomes
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "title" : "Some configuration of the node. This does not need to be complete against the
 configuration schema."
}
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action AuthLevelDecision --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query AuthLevelDecision --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read AuthLevelDecision --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update AuthLevelDecision --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "authLevelRequirement" : {
      "title" : "Sufficient Authentication Level",
      "description" : "The current authentication level must be greater than or equal to this value
 for the decision to return true.",
      "propertyOrder" : 100,
      "type" : "integer",
      "exampleValue" : ""
    }
  },
  "required" : [ "authLevelRequirement" ]
}
```

AuthTree

Realm Operations

Authentication trees.

Resource path: `/realm-config/authentication/authenticationtrees/trees`

Resource version: `1.0`

clone

Creates a new tree and underlying set of nodes with the same node configurations as the cloned tree.

Usage:

```
am> action AuthTree --realm Realm --body body --actionName clone
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "newId" : {
      "type" : "string",
      "title" : "New Tree ID",
      "description" : "The ID for the tree that will be created."
    }
  }
}
```

create

Usage:

```
am> create AuthTree --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "description" : "A tree contains a set of nodes and their connections.",
  "type" : "object",
  "title" : "Authentication Tree",
  "properties" : {
    "description" : {
      "type" : "string",
      "title" : "Description",
      "description" : "A description of the tree."
    },
    "nodes" : {
      "type" : "object",
      "title" : "Nodes",
      "description" : "A map of node ID to node association details.",
      "patternProperties" : {
        ".*" : {
          "type" : "object",
          "title" : "Node",
          "description" : "A association of a node with a tree.",
          "properties" : {
            "connections" : {
              "type" : "object",
              "title" : "Connections",
              "description" : "The node's connected outcomes.",
              "patternProperties" : {
                ".*" : {
                  "type" : "string",
                  "title" : "Node ID",
                  "description" : "The ID of the node that this outcome connects to."
```

```
              }
            }
          },
          "x" : {
            "type" : "string",
            "title" : "tree.node.x",
            "description" : "tree.node.x.description"
          },
          "y" : {
            "type" : "string",
            "title" : "tree.node.y",
            "description" : "tree.node.y.description"
          },
          "_outcomes" : {
            "type" : "array",
            "title" : "Outcomes",
            "description" : "The node's complete set of outcomes.",
            "readOnly" : true,
            "items" : {
              "type" : "object",
              "title" : "Outcome",
              "description" : "A possible outcome of the node.",
              "readOnly" : true,
              "properties" : {
                "id" : {
                  "type" : "string",
                  "title" : "ID",
                  "description" : "The identifier of the outcome.",
                  "readOnly" : true
                },
                "displayName" : {
                  "type" : "string",
                  "title" : "Display Name",
                  "description" : "The display name of the outcome, in the requester's preferred
locale.",
                  "readOnly" : true
                }
              }
            }
          }
        }
      }
    }
  },
  "staticNodes" : {
    "type" : "object",
    "title" : "Static Nodes",
    "description" : "A map of node ID to node layout positions for the static nodes, start, success
and failure.",
    "patternProperties" : {
      ".*" : {
        "type" : "object",
        "title" : "Node",
        "description" : "A association of a node with a tree.",
        "properties" : {
          "x" : {
            "type" : "string",
            "title" : "tree.node.x",
            "description" : "tree.node.x.description"
```

```
            },
            "y" : {
              "type" : "string",
              "title" : "tree.node.y",
              "description" : "tree.node.y.description"
            }
          }
        }
      }
    },
    "uiConfig" : {
      "type" : "object",
      "title" : "UI Configuration",
      "description" : "Optional key-value map to hold implementation-specific client properties.",
      "patternProperties" : {
        ".*" : {
          "type" : "string"
        }
      }
    },
    "identityResource" : {
      "type" : "string",
      "title" : "Identity Resource",
      "description" : "Optional IDM identity resource, e.g. managed/user."
    }
  }
}
```

delete

Usage:

```
am> delete AuthTree --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action AuthTree --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action AuthTree --realm Realm --actionName getCreatableTypes
```

getIds

Get the names of each tree configured in this realm.

Usage:

```
am> action AuthTree --realm Realm --actionName getIds
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action AuthTree --realm Realm --actionName nextdescendents
```

query

Query for all authentication trees. Only a query filter of 'true' is supported.

Usage:

```
am> query AuthTree --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read AuthTree --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update AuthTree --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "description" : "A tree contains a set of nodes and their connections.",
  "type" : "object",
  "title" : "Authentication Tree",
  "properties" : {
    "description" : {
      "type" : "string",
      "title" : "Description",
      "description" : "A description of the tree."
    },
    "nodes" : {
      "type" : "object",
      "title" : "Nodes",
      "description" : "A map of node ID to node association details.",
      "patternProperties" : {
        ".*" : {
          "type" : "object",
          "title" : "Node",
          "description" : "A association of a node with a tree.",
          "properties" : {
            "connections" : {
              "type" : "object",
              "title" : "Connections",
              "description" : "The node's connected outcomes.",
              "patternProperties" : {
                ".*" : {
                  "type" : "string",
                  "title" : "Node ID",
                  "description" : "The ID of the node that this outcome connects to."
                }
              }
            },
            "x" : {
              "type" : "string",
              "title" : "tree.node.x",
              "description" : "tree.node.x.description"
            },
            "y" : {
              "type" : "string",
              "title" : "tree.node.y",
              "description" : "tree.node.y.description"
            },
            "_outcomes" : {
              "type" : "array",
              "title" : "Outcomes",
              "description" : "The node's complete set of outcomes.",
              "readOnly" : true,
              "items" : {
                "type" : "object",
```

```
                "title" : "Outcome",
                "description" : "A possible outcome of the node.",
                "readOnly" : true,
                "properties" : {
                  "id" : {
                    "type" : "string",
                    "title" : "ID",
                    "description" : "The identifier of the outcome.",
                    "readOnly" : true
                  },
                  "displayName" : {
                    "type" : "string",
                    "title" : "Display Name",
                    "description" : "The display name of the outcome, in the requester's preferred
locale.",
                    "readOnly" : true
                  }
                }
              }
            }
          }
        }
      }
    },
    "staticNodes" : {
      "type" : "object",
      "title" : "Static Nodes",
      "description" : "A map of node ID to node layout positions for the static nodes, start, success
and failure.",
      "patternProperties" : {
        ".*" : {
          "type" : "object",
          "title" : "Node",
          "description" : "A association of a node with a tree.",
          "properties" : {
            "x" : {
              "type" : "string",
              "title" : "tree.node.x",
              "description" : "tree.node.x.description"
            },
            "y" : {
              "type" : "string",
              "title" : "tree.node.y",
              "description" : "tree.node.y.description"
            }
          }
        }
      }
    },
    "uiConfig" : {
      "type" : "object",
      "title" : "UI Configuration",
      "description" : "Optional key-value map to hold implementation-specific client properties.",
      "patternProperties" : {
        ".*" : {
          "type" : "string"
        }
      }
    },
```

```
    "identityResource" : {
      "type" : "string",
      "title" : "Identity Resource",
      "description" : "Optional IDM identity resource, e.g. managed/user."
    }
  }
}
```

validate

Validates a tree giving errors and warnings.

Usage:

```
am> action AuthTree --realm Realm --body body --actionName validate
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "description" : "A tree contains a set of nodes and their connections.",
  "type" : "object",
  "title" : "Authentication Tree",
  "properties" : {
    "description" : {
      "type" : "string",
      "title" : "Description",
      "description" : "A description of the tree."
    },
    "nodes" : {
      "type" : "object",
      "title" : "Nodes",
      "description" : "A map of node ID to node association details.",
      "patternProperties" : {
        ".*" : {
          "type" : "object",
          "title" : "Node",
          "description" : "A association of a node with a tree.",
          "properties" : {
            "connections" : {
              "type" : "object",
              "title" : "Connections",
              "description" : "The node's connected outcomes.",
              "patternProperties" : {
                ".*" : {
                  "type" : "string",
                  "title" : "Node ID",
                  "description" : "The ID of the node that this outcome connects to."
                }
              }
            },
            "x" : {
              "type" : "string",
              "title" : "tree.node.x",
```

```
            "description" : "tree.node.x.description"
          },
          "y" : {
            "type" : "string",
            "title" : "tree.node.y",
            "description" : "tree.node.y.description"
          },
          "_outcomes" : {
            "type" : "array",
            "title" : "Outcomes",
            "description" : "The node's complete set of outcomes.",
            "readOnly" : true,
            "items" : {
              "type" : "object",
              "title" : "Outcome",
              "description" : "A possible outcome of the node.",
              "readOnly" : true,
              "properties" : {
                "id" : {
                  "type" : "string",
                  "title" : "ID",
                  "description" : "The identifier of the outcome.",
                  "readOnly" : true
                },
                "displayName" : {
                  "type" : "string",
                  "title" : "Display Name",
                  "description" : "The display name of the outcome, in the requester's preferred
locale.",
                  "readOnly" : true
                }
              }
            }
          }
        }
      }
    },
    "staticNodes" : {
      "type" : "object",
      "title" : "Static Nodes",
      "description" : "A map of node ID to node layout positions for the static nodes, start, success
and failure.",
      "patternProperties" : {
        ".*" : {
          "type" : "object",
          "title" : "Node",
          "description" : "A association of a node with a tree.",
          "properties" : {
            "x" : {
              "type" : "string",
              "title" : "tree.node.x",
              "description" : "tree.node.x.description"
            },
            "y" : {
              "type" : "string",
              "title" : "tree.node.y",
              "description" : "tree.node.y.description"
            }
```

```
          }
        }
      }
    },
    "uiConfig" : {
      "type" : "object",
      "title" : "UI Configuration",
      "description" : "Optional key-value map to hold implementation-specific client properties.",
      "patternProperties" : {
        ".*" : {
          "type" : "string"
        }
      }
    },
    "identityResource" : {
      "type" : "string",
      "title" : "Identity Resource",
      "description" : "Optional IDM identity resource, e.g. managed/user."
    }
  }
}
```

AuthenticateThing

Realm Operations

Resource path: `/realm-config/authentication/authenticationtrees/nodes/IotAuthenticationNode`

Resource version: `1.0`

create

Usage:

```
am> create AuthenticateThing --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "required" : [ ]
}
```

delete

Usage:

```
am> delete AuthenticateThing --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action AuthenticateThing --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action AuthenticateThing --realm Realm --actionName getCreatableTypes
```

listOutcomes

List the available outcomes for the node type.

Usage:

```
am> action AuthenticateThing --realm Realm --body body --actionName listOutcomes
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "title" : "Some configuration of the node. This does not need to be complete against the
 configuration schema."
}
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action AuthenticateThing --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query AuthenticateThing --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read AuthenticateThing --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update AuthenticateThing --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "required" : [ ]
}
```

Authentication

Realm Operations

Resource path: `/realm-config/authentication`

Resource version: `1.0`

create

Usage:

```
am> create Authentication --realm Realm --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "accountlockout" : {
      "type" : "object",
      "title" : "Account Lockout",
      "propertyOrder" : 2,
      "properties" : {
        "lockoutDuration" : {
          "title" : "Login Failure Lockout Duration",
          "description" : "The duration of the users account lockout, in minutes.<br><br>OpenAM can
 either lockout the users account indefinitely (until administration action) by setting the duration
 to 0, (the default) or OpenAM can lock the users account for a given number of minutes. After the
 lockout interval, the user will be able to successfully authenticate to OpenAM.",
          "propertyOrder" : 1300,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "loginFailureLockoutMode" : {
          "title" : "Login Failure Lockout Mode",
          "description" : "Enables account lockout functionality for users authenticating to this
 realm.<br><br>OpenAM can track the number of failed authentications by a user over time and if a pre-
defined limit is breached, OpenAM can lockout the users account and perform additional functions.<br/
><br/><i>NB </i>This functionality is in addition to any account lockout behaviour implemented by the
 LDAP Directory Server.",
          "propertyOrder" : 800,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "lockoutDurationMultiplier" : {
          "title" : "Lockout Duration Multiplier",
```

```
          "description" : "Value multiplied to the Login Failure Lockout Duration for each successive
 lockout.<br><br>This property is used to enable OpenAM to increase the account lockout duration for
 each successive account lockout. For example: If the lockout duration is set to 10 and the duration
 multiplier is set to 2; the duration of the first lockout will be 10 minutes and the duration of the
 second lockout will be 20 minutes.<br/><br/>The default value of 1 disables this function.  ",
          "propertyOrder" : 1400,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "loginFailureCount" : {
          "title" : "Login Failure Lockout Count",
          "description" : "The maximum number of failed authentications for a user before their
 account is locked.<br><br>This setting controls the maximum number of failed authentications a user
 can have during the lockout interval before OpenAM locks the users account.",
          "propertyOrder" : 900,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "lockoutAttributeName" : {
          "title" : "Lockout Attribute Name",
          "description" : "Name of custom lockout attribute <br><br>When OpenAM locks an account, the
 <code>inetuserstatus</code> attribute in the locked account is set to Inactive. In addition, OpenAM
 can set the value of another attribute in the users profile. ",
          "propertyOrder" : 1500,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "lockoutEmailAddress" : {
          "title" : "Email Address to Send Lockout Notification",
          "description" : "An email address or set of email addresses that receive notifications
 about account lockout events.<br><br>OpenAM can be configured to send a localisable email
 message to a set of email addresses when account lockout events occur. The contents of the
 email message is configured using the following properties in the <code>amAuth.properties</code>
 file.<br/><ul><li><code>lockOutEmailFrom</code> : The \"From\" address of the email message</
li><li><code>lockOutEmailSub</code> : The subject of the email message</li><li><code>lockOutEmailMsg</
code> : The contents of the email message</li></ul><br/>The identity for whom the account has
 been locked is included in the email message.<br/><br/>The format of this property is:<br/
><code>emailaddress|locale|charset</code>. Multiple email addresses are space-separated.<br/>Email
 addresses must include the domain name, such as <code>admin@example.com</code>.",
          "propertyOrder" : 1100,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "storeInvalidAttemptsInDataStore" : {
          "title" : "Store Invalid Attempts in Data Store",
          "description" : "Enables sharing of login failure attempts across AM Instances<br><br>When
 this setting is enabled AM will store the user's invalid authentication information in the data store
 under the attribute configured in the <i>Invalid Attempts Data Attribute Name</i> property. This
 setting only applies to authentication modules and chains; authentication trees will <i>always</i>
 write their account lockout progress and status to the data store.",
          "propertyOrder" : 2700,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
```

```
       "lockoutWarnUserCount" : {
         "title" : "Warn User After N Failures",
         "description" : "Warn the user when they reach this level of failed
authentications.<br><br>The user will be given a warning when they reach this level of failed
authentications during the lockout interval.<br/>The text of the lockout warning is configured using
the <code>lockOutWarning</code> property in the <code>amAuth.properties</code> file.",
         "propertyOrder" : 1200,
         "required" : true,
         "type" : "integer",
         "exampleValue" : ""
       },
       "invalidAttemptsDataAttributeName" : {
         "title" : "Invalid Attempts Data Attribute Name",
         "description" : "The name of the attribute used to store information about failed
authentications.<br><br>OpenAM can be configured to store information about invalid authentications
in the users profile. This allows multiple instances of OpenAM in the same site to share
information about a users invalid authentication attempts. By default the custom attribute;
<code>sunAMAuthInvalidAttemptsData</code> defined in the <code>sunAMAuthAccountLockout</code>
objectclass is used to store this data. Use this property to change the attribute used by OpenAM to
store this information.<br/><br/><i>NB </i>Any attribute specified must be a valid attribute in the
data store.",
         "propertyOrder" : 1700,
         "required" : true,
         "type" : "string",
         "exampleValue" : ""
       },
       "lockoutAttributeValue" : {
         "title" : "Lockout Attribute Value",
         "description" : "Value to set in custom lockout attribute<br><br>This is the value that will
be set on the custom attribute in the users profile when they account is locked.",
         "propertyOrder" : 1600,
         "required" : true,
         "type" : "string",
         "exampleValue" : ""
       },
       "loginFailureDuration" : {
         "title" : "Login Failure Lockout Interval",
         "description" : "The lockout interval time is in minutes.<br><br>OpenAM tracks the failed
authentication count for a user over the lockout interval.<br/><br/>For example: If the lockout
interval is 5 minutes and the lockout count is 5; the user will have to have failed to authenticate
5 times over the previous 5 minutes for the account to be locked. Failed authentications the occurred
outside of the 5 minute interval are ignored.",
         "propertyOrder" : 1000,
         "required" : true,
         "type" : "integer",
         "exampleValue" : ""
       }
     }
   },
   "postauthprocess" : {
     "type" : "object",
     "title" : "Post Authentication Processing",
     "propertyOrder" : 6,
     "properties" : {
       "loginSuccessUrl" : {
         "title" : "Default Success Login URL",
         "description" : "Successful logins will be forwarded to this URL<br><br>This is the URL to
which clients will be forwarded upon successful authentication. Enter a URL or URI relative to the
```

```
local OpenAM. URL or URI can be prefixed with the ClientType|URL if client specific. URL without
http(s) protocol will be appended to the current URI of OpenAM.",
         "propertyOrder" : 1800,
         "required" : true,
         "items" : {
           "type" : "string"
         },
         "type" : "array",
         "exampleValue" : ""
       },
       "usernameGeneratorClass" : {
         "title" : "Pluggable User Name Generator Class",
         "description" : "The name of the default implementation of the user name
generator class.<br><br>The name of the class used to return a list of usernames to
the Membership auth module.<br/><br/><i>NB </i>This class must implement the interface
<code>com.sun.identity.authentication.spi.UserIDGenerator</code>",
         "propertyOrder" : 2200,
         "required" : true,
         "type" : "string",
         "exampleValue" : ""
       },
       "loginFailureUrl" : {
         "title" : "Default Failure Login URL ",
         "description" : "Failed logins will be forwarded to this URL<br><br>This is the URL to
which clients will be forwarded upon failed authentication. Enter a URL or URI relative to the
local OpenAM. URL or URI can be prefixed with ClientType|URL if client specific. URL without http(s)
protocol will be appended to the current URI of OpenAM.",
         "propertyOrder" : 1900,
         "required" : true,
         "items" : {
           "type" : "string"
         },
         "type" : "array",
         "exampleValue" : ""
       },
       "usernameGeneratorEnabled" : {
         "title" : "Generate UserID Mode",
         "description" : "Enables this mode in the Membership auth module.<br><br>When this mode is
enabled, if the Membership auth module detects that the supplied username already exists in the data
store then a list of valid usernames can be shown to the user, if requested by said user.",
         "propertyOrder" : 2100,
         "required" : true,
         "type" : "boolean",
         "exampleValue" : ""
       },
       "loginPostProcessClass" : {
         "title" : "Authentication Post Processing Classes",
         "description" : "A list of post authentication processing classes for all users
in this realm.<br><br>This is a list of Post Processing Classes that will be called by
OpenAM for all users that authenticate to this realm. Refer to the documentation for the
places where the list of post authentication classes can be set and their precedence.
<br/><br/>For example: org.forgerock.auth.PostProcessClass<br/><i>NB </i>OpenAM must be
able to find these classes on the <code>CLASSPATH</code> and must implement the interface
<code>com.sun.identity.authentication.spi.AMPostAuthProcessInterface</code>.",
         "propertyOrder" : 2000,
         "required" : true,
         "items" : {
           "type" : "string"
         },
```

```
          "type" : "array",
          "exampleValue" : ""
        },
        "userAttributeSessionMapping" : {
          "title" : "User Attribute Mapping to Session Attribute",
          "description" : "Mapping of user profile attribute name to session attribute
 name.<br><br>The setting causes OpenAM to read the named attributes from the users profile in the
 data store and store their values in the users session.<br/></br>Format: User Profile Attribute|
Session Attribute name. ",
          "propertyOrder" : 3000,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        }
      }
    },
    "trees" : {
      "type" : "object",
      "title" : "Trees",
      "propertyOrder" : 4,
      "properties" : {
        "authenticationSessionsMaxDuration" : {
          "title" : "Max duration (minutes)",
          "description" : "Specify how long an authentication session can last.<br><br>From the time
 an authentication session is generated, the session will be invalid after this number of minutes.
 Values from <strong>1</strong> upwards are allowed.",
          "propertyOrder" : 3860,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "authenticationSessionsStateManagement" : {
          "title" : "Authentication session state management scheme",
          "description" : "Specify how the authentication session state is managed.<br><br>CTS option
 will write the state down to the underlying core token store.<br />JWT option will transmit the
 state in a JWT to the client.<br />In-Memory option will maintain the state in the memory (requires
 sticky loadbalancing).<br /><br /> <em>To configure JWT signing, encryption, and blacklisting use the
 options in the Client-based Sessions section of the Sessions global service.</em>",
          "propertyOrder" : 3850,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "authenticationSessionsWhitelist" : {
          "title" : "Enable whitelisting",
          "description" : "Enables explicit whitelisting of valid authentication states to prevent
 replay attacks.<br><br>If enabled, each time a response is sent to the user a randomly generated
 state parameter is also sent back to user. This state parameter is stored accessible to AM and
 must be sent in with the subsequent request. After a request has been received with a valid state
 parameter, the next response contains a new state, and the server's view of the valid state parameter
 is updated.",
          "propertyOrder" : 3880,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
```

```
       "suspendedAuthenticationTimeout" : {
         "title" : "Suspended authentication duration (minutes)",
         "description" : "Specify how long a suspended authentication session can last.<br><br>From
 the time a suspended authentication session is generated, the session will be invalid after this
 number of minutes. Values from <strong>1</strong> upwards are allowed. This timeout should be less
 than or equal to the authentication sessionâ##s timeout value.",
         "propertyOrder" : 3870,
         "required" : true,
         "type" : "integer",
         "exampleValue" : ""
       }
     }
   },
   "general" : {
     "type" : "object",
     "title" : "General",
     "propertyOrder" : 3,
     "properties" : {
       "statelessSessionsEnabled" : {
         "title" : "Use Client-based Sessions",
         "description" : "Enables client-based sessions.<br><br>Client-based sessions provide elastic
 scalability by storing all session state as a JWT in a cookie stored on the client. It is highly
 recommended to enable signing and encryption of the JWT in the global session service.",
         "propertyOrder" : 3800,
         "required" : true,
         "type" : "boolean",
         "exampleValue" : ""
       },
       "locale" : {
         "title" : "Default Authentication Locale",
         "description" : "",
         "propertyOrder" : 600,
         "required" : true,
         "type" : "string",
         "exampleValue" : ""
       },
       "userStatusCallbackPlugins" : {
         "title" : "Pluggable User Status Event Classes",
         "description" : "List of classes to be called when status of the user account
 changes.<br><br>When the status of a users account changes, OpenAM can be configured to call into
 a custom class. The custom class can then be used to perform some action as required. The built in
 status change events are:<br/><br/><ul><li>Account locked</li><li>Password changed</li></ul><br/
>Custom code can also extend this mechanism.",
         "propertyOrder" : 2600,
         "required" : true,
         "items" : {
           "type" : "string"
         },
         "type" : "array",
         "exampleValue" : ""
       },
       "identityType" : {
         "title" : "Identity Types",
         "description" : "",
         "propertyOrder" : 2500,
         "required" : true,
         "items" : {
           "type" : "string"
         },
```

```
          "type" : "array",
          "exampleValue" : ""
        },
        "defaultAuthLevel" : {
          "title" : "Default Authentication Level",
          "description" : "The default authentication level for modules in this realm.<br><br>If
the authentication module does not set it's own auth level then the module will have the default
authentication level for the realm.",
          "propertyOrder" : 4100,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "externalLoginPageUrl" : {
          "title" : "External Login Page URL",
          "description" : "Link to the external login user interface.<br><br>If the authentication
user interface is hosted separately from AM, its URL can be provided here. AM will use this
URL for example when it's constructing the resume URI in case authentication is suspended in an
authentication tree.",
          "propertyOrder" : 3910,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "twoFactorRequired" : {
          "title" : "Two Factor Authentication Mandatory",
          "description" : "Enforces ALL 2FA (OATH and Push) authentication Modules (not nodes) only
for this authentication realm.",
          "propertyOrder" : 3900,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        }
      }
    },
    "core" : {
      "type" : "object",
      "title" : "Core",
      "propertyOrder" : -1,
      "properties" : {
        "orgConfig" : {
          "title" : "Organization Authentication Configuration",
          "description" : "Default Authentication Service for users<br><br>This is the authentication
service that will be used to authenticate users to this realm.",
          "propertyOrder" : 700,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "adminAuthModule" : {
          "title" : "Administrator Authentication Configuration",
          "description" : "Default Authentication Service for administrators<br><br>This is the
authentication service that will be used to authentication administrative users to this realm.",
          "propertyOrder" : 200,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      }
```

```
   },
   "security" : {
     "type" : "object",
     "title" : "Security",
     "propertyOrder" : 5,
     "properties" : {
       "zeroPageLoginEnabled" : {
         "title" : "Zero Page Login",
         "description" : "Allows a user to authenticate using GET request parameters without
showing the login screen.<br><br>Enable this feature if the authentication mechanism uses a single
authentication screen or the first authentication screen should always be invisible to users (since
it is auto-submitted). Use caution when enabling this feature as it can be used to authenticate using
regular GET parameters, which could be cached by browsers and logged in server and proxy access logs
exposing the values of the GET parameters.",
         "propertyOrder" : 3400,
         "required" : true,
         "type" : "boolean",
         "exampleValue" : ""
       },
       "moduleBasedAuthEnabled" : {
         "title" : "Module Based Authentication",
         "description" : "Allows a user to authenticate via module based authentication.<br><br>The
feature allow users to override the realm configuration and use a named authentication module to
authenticate.<br/><br/><i>NB </i>Recommended to turn this feature off in production environments.",
         "propertyOrder" : 2800,
         "required" : true,
         "type" : "boolean",
         "exampleValue" : ""
       },
       "sharedSecret" : {
         "title" : "Organization Authentication Signing Secret",
         "description" : "HMAC shared secret for signing RESTful Authentication requests.<br><br>This
is the shared secret for signing state used in RESTful authentication requests. Should be at Base-64
encoded and at least 128-bits in length. By default a cryptographically secure random value is
generated.",
         "propertyOrder" : 4000,
         "required" : true,
         "type" : "string",
         "format" : "password",
         "exampleValue" : ""
       },
       "zeroPageLoginAllowedWithoutReferrer" : {
         "title" : "Zero Page Login Allowed without Referer?",
         "description" : "Whether to allow Zero Page Login if the HTTP Referer header is
missing.<br><br>The HTTP Referer header is sometimes missing from requests (e.g., if making a request
to HTTP from HTTPS). This setting controls whether such requests should be allowed or not. Setting
to 'true' will reduce the risk of Login CSRF attacks with Zero Page Login, but may potentially deny
legitimate requests.",
         "propertyOrder" : 3700,
         "required" : true,
         "type" : "boolean",
         "exampleValue" : ""
       },
       "zeroPageLoginReferrerWhiteList" : {
         "title" : "Zero Page Login Referer Whitelist",
         "description" : "List of allowed HTTP Referer (sic) URLs from which Zero Page Login requests
are allowed.<br><br>Enter here all URLs from which you want to allow Zero Page Login. This provides
some mitigation against Login CSRF attacks. Leave empty to allow from any Referer. Applies to both
GET and POST login requests.",
```

```
          "propertyOrder" : 3600,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "keyAlias" : {
          "title" : "Persistent Cookie Encryption Certificate Alias",
          "description" : "Keystore Alias for encrypting Persistent Cookies.<br><br>This is the alias
for the private/public keys in the Keystore used in Persistent Cookie authentication requests.",
          "propertyOrder" : 3300,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "userprofile" : {
      "type" : "object",
      "title" : "User Profile",
      "propertyOrder" : 0,
      "properties" : {
        "aliasAttributeName" : {
          "title" : "Alias Search Attribute Name",
          "description" : "The secondary LDAP attribute retrieves the user profile if the primary
LDAP attribute specified in 'User Naming Attribute' fails.<br><br>This list of LDAP attributes
is used to extend the set of attributes searched by OpenAM to find the users profile.<br>For
example: <ul><li>cn</li><li>mail</li><li>givenname</li></ul><br/>A user authenticates to OpenAM
under the id of steve, OpenAM will first search using the naming attribute (uid by default) so
uid=steve, if no match is found then cn=steve will be searched until a match is found or the list is
exhausted.<br><br/><br/><i>NB </i> Only used when User Profile searching is enabled.",
          "propertyOrder" : 400,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "defaultRole" : {
          "title" : "User Profile Dynamic Creation Default Roles",
          "description" : "List of roles of which dynamically created users will be a
member.<br><br>Enter the DN for each role that will be assigned to a new user when their profile has
been dynamically created by OpenAM.<br/><br/><i>NB </i> Deprecated functionality in OpenAM.",
          "propertyOrder" : 300,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "dynamicProfileCreation" : {
          "title" : "User Profile",
          "description" : "Controls the result of the user profile success post successful
authentication.<br><br>Controls whether a user profile is required for authentication to be
```

```
 successful or if the profile will be dynamically created if none already exists. Choose ignore if you
 do not have a data store configured in the realm.",
          "propertyOrder" : 100,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    }
  }
}
```

delete

Usage:

```
am> delete Authentication --realm Realm
```

read

Usage:

```
am> read Authentication --realm Realm
```

update

Usage:

```
am> update Authentication --realm Realm --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "accountlockout" : {
      "type" : "object",
      "title" : "Account Lockout",
      "propertyOrder" : 2,
      "properties" : {
        "lockoutDuration" : {
          "title" : "Login Failure Lockout Duration",
          "description" : "The duration of the users account lockout, in minutes.<br><br>OpenAM can
 either lockout the users account indefinitely (until administration action) by setting the duration
 to 0, (the default) or OpenAM can lock the users account for a given number of minutes. After the
 lockout interval, the user will be able to successfully authenticate to OpenAM.",
          "propertyOrder" : 1300,
          "required" : true,
```

```
          "type" : "integer",
          "exampleValue" : ""
        },
        "loginFailureLockoutMode" : {
          "title" : "Login Failure Lockout Mode",
          "description" : "Enables account lockout functionality for users authenticating to this
 realm.<br><br>OpenAM can track the number of failed authentications by a user over time and if a pre-
defined limit is breached, OpenAM can lockout the users account and perform additional functions.<br/
><br/><i>NB </i>This functionality is in addition to any account lockout behaviour implemented by the
 LDAP Directory Server.",
          "propertyOrder" : 800,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "lockoutDurationMultiplier" : {
          "title" : "Lockout Duration Multiplier",
          "description" : "Value multiplied to the Login Failure Lockout Duration for each successive
 lockout.<br><br>This property is used to enable OpenAM to increase the account lockout duration for
 each successive account lockout. For example: If the lockout duration is set to 10 and the duration
 multiplier is set to 2; the duration of the first lockout will be 10 minutes and the duration of the
 second lockout will be 20 minutes.<br/><br/>The default value of 1 disables this function.  ",
          "propertyOrder" : 1400,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "loginFailureCount" : {
          "title" : "Login Failure Lockout Count",
          "description" : "The maximum number of failed authentications for a user before their
 account is locked.<br><br>This setting controls the maximum number of failed authentications a user
 can have during the lockout interval before OpenAM locks the users account.",
          "propertyOrder" : 900,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "lockoutAttributeName" : {
          "title" : "Lockout Attribute Name",
          "description" : "Name of custom lockout attribute <br><br>When OpenAM locks an account, the
 <code>inetuserstatus</code> attribute in the locked account is set to Inactive. In addition, OpenAM
 can set the value of another attribute in the users profile. ",
          "propertyOrder" : 1500,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "lockoutEmailAddress" : {
          "title" : "Email Address to Send Lockout Notification",
          "description" : "An email address or set of email addresses that receive notifications
 about account lockout events.<br><br>OpenAM can be configured to send a localisable email
 message to a set of email addresses when account lockout events occur. The contents of the
 email message is configured using the following properties in the <code>amAuth.properties</code>
 file.<br/><ul><li><code>lockOutEmailFrom</code> : The \"From\" address of the email message</
li><li><code>lockOutEmailSub</code> : The subject of the email message</li><li><code>lockOutEmailMsg</
code> : The contents of the email message</li></ul><br/>The identity for whom the account has
 been locked is included in the email message.<br/><br/>The format of this property is:<br/
><code>emailaddress|locale|charset</code>. Multiple email addresses are space-separated.<br/>Email
 addresses must include the domain name, such as <code>admin@example.com</code>.",
```

```
          "propertyOrder" : 1100,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "storeInvalidAttemptsInDataStore" : {
          "title" : "Store Invalid Attempts in Data Store",
          "description" : "Enables sharing of login failure attempts across AM Instances<br><br>When
this setting is enabled AM will store the user's invalid authentication information in the data store
under the attribute configured in the <i>Invalid Attempts Data Attribute Name</i> property. This
setting only applies to authentication modules and chains; authentication trees will <i>always</i>
write their account lockout progress and status to the data store.",
          "propertyOrder" : 2700,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "lockoutWarnUserCount" : {
          "title" : "Warn User After N Failures",
          "description" : "Warn the user when they reach this level of failed
authentications.<br><br>The user will be given a warning when they reach this level of failed
authentications during the lockout interval.<br/>The text of the lockout warning is configured using
the <code>lockOutWarning</code> property in the <code>amAuth.properties</code> file.",
          "propertyOrder" : 1200,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "invalidAttemptsDataAttributeName" : {
          "title" : "Invalid Attempts Data Attribute Name",
          "description" : "The name of the attribute used to store information about failed
authentications.<br><br>OpenAM can be configured to store information about invalid authentications
in the users profile. This allows multiple instances of OpenAM in the same site to share
information about a users invalid authentication attempts. By default the custom attribute;
<code>sunAMAuthInvalidAttemptsData</code> defined in the <code>sunAMAuthAccountLockout</code>
objectclass is used to store this data. Use this property to change the attribute used by OpenAM to
store this information.<br/><br/><i>NB </i>Any attribute specified must be a valid attribute in the
data store.",
          "propertyOrder" : 1700,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "lockoutAttributeValue" : {
          "title" : "Lockout Attribute Value",
          "description" : "Value to set in custom lockout attribute<br><br>This is the value that will
be set on the custom attribute in the users profile when they account is locked.",
          "propertyOrder" : 1600,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "loginFailureDuration" : {
          "title" : "Login Failure Lockout Interval",
          "description" : "The lockout interval time is in minutes.<br><br>OpenAM tracks the failed
authentication count for a user over the lockout interval.<br/><br/>For example: If the lockout
interval is 5 minutes and the lockout count is 5; the user will have to have failed to authenticate
5 times over the previous 5 minutes for the account to be locked. Failed authentications the occurred
outside of the 5 minute interval are ignored.",
```

```
          "propertyOrder" : 1000,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        }
      }
    },
    "postauthprocess" : {
      "type" : "object",
      "title" : "Post Authentication Processing",
      "propertyOrder" : 6,
      "properties" : {
        "loginSuccessUrl" : {
          "title" : "Default Success Login URL",
          "description" : "Successful logins will be forwarded to this URL<br><br>This is the URL to
which clients will be forwarded upon successful authentication. Enter a URL or URI relative to the
local OpenAM. URL or URI can be prefixed with the ClientType|URL if client specific. URL without
http(s) protocol will be appended to the current URI of OpenAM.",
          "propertyOrder" : 1800,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "usernameGeneratorClass" : {
          "title" : "Pluggable User Name Generator Class",
          "description" : "The name of the default implementation of the user name
generator class.<br><br>The name of the class used to return a list of usernames to
the Membership auth module.<br/><br/><i>NB </i>This class must implement the interface
<code>com.sun.identity.authentication.spi.UserIDGenerator</code>",
          "propertyOrder" : 2200,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "loginFailureUrl" : {
          "title" : "Default Failure Login URL ",
          "description" : "Failed logins will be forwarded to this URL<br><br>This is the URL to
which clients will be forwarded upon failed authentication. Enter a URL or URI relative to the
local OpenAM. URL or URI can be prefixed with ClientType|URL if client specific. URL without http(s)
protocol will be appended to the current URI of OpenAM.",
          "propertyOrder" : 1900,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "usernameGeneratorEnabled" : {
          "title" : "Generate UserID Mode",
          "description" : "Enables this mode in the Membership auth module.<br><br>When this mode is
enabled, if the Membership auth module detects that the supplied username already exists in the data
store then a list of valid usernames can be shown to the user, if requested by said user.",
          "propertyOrder" : 2100,
          "required" : true,
          "type" : "boolean",
```

```
          "exampleValue" : ""
        },
        "loginPostProcessClass" : {
          "title" : "Authentication Post Processing Classes",
          "description" : "A list of post authentication processing classes for all users
 in this realm.<br><br>This is a list of Post Processing Classes that will be called by
 OpenAM for all users that authenticate to this realm. Refer to the documentation for the
 places where the list of post authentication classes can be set and their precedence.
 <br/><br/>For example: org.forgerock.auth.PostProcessClass<br/><i>NB </i>OpenAM must be
 able to find these classes on the <code>CLASSPATH</code> and must implement the interface
 <code>com.sun.identity.authentication.spi.AMPostAuthProcessInterface</code>.",
          "propertyOrder" : 2000,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "userAttributeSessionMapping" : {
          "title" : "User Attribute Mapping to Session Attribute",
          "description" : "Mapping of user profile attribute name to session attribute
 name.<br><br>The setting causes OpenAM to read the named attributes from the users profile in the
 data store and store their values in the users session.<br/></br>Format: User Profile Attribute|
Session Attribute name. ",
          "propertyOrder" : 3000,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        }
      }
    },
    "trees" : {
      "type" : "object",
      "title" : "Trees",
      "propertyOrder" : 4,
      "properties" : {
        "authenticationSessionsMaxDuration" : {
          "title" : "Max duration (minutes)",
          "description" : "Specify how long an authentication session can last.<br><br>From the time
 an authentication session is generated, the session will be invalid after this number of minutes.
 Values from <strong>1</strong> upwards are allowed.",
          "propertyOrder" : 3860,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "authenticationSessionsStateManagement" : {
          "title" : "Authentication session state management scheme",
          "description" : "Specify how the authentication session state is managed.<br><br>CTS option
 will write the state down to the underlying core token store.<br />JWT option will transmit the
 state in a JWT to the client.<br />In-Memory option will maintain the state in the memory (requires
 sticky loadbalancing).<br /><br /> <em>To configure JWT signing, encryption, and blacklisting use the
 options in the Client-based Sessions section of the Sessions global service.</em>",
          "propertyOrder" : 3850,
          "required" : true,
```

```
          "type" : "string",
          "exampleValue" : ""
        },
        "authenticationSessionsWhitelist" : {
          "title" : "Enable whitelisting",
          "description" : "Enables explicit whitelisting of valid authentication states to prevent
 replay attacks.<br><br>If enabled, each time a response is sent to the user a randomly generated
 state parameter is also sent back to user. This state parameter is stored accessible to AM and
 must be sent in with the subsequent request. After a request has been received with a valid state
 parameter, the next response contains a new state, and the server's view of the valid state parameter
 is updated.",
          "propertyOrder" : 3880,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "suspendedAuthenticationTimeout" : {
          "title" : "Suspended authentication duration (minutes)",
          "description" : "Specify how long a suspended authentication session can last.<br><br>From
 the time a suspended authentication session is generated, the session will be invalid after this
 number of minutes. Values from <strong>1</strong> upwards are allowed. This timeout should be less
 than or equal to the authentication sessionâ##s timeout value.",
          "propertyOrder" : 3870,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        }
      }
    },
    "general" : {
      "type" : "object",
      "title" : "General",
      "propertyOrder" : 3,
      "properties" : {
        "statelessSessionsEnabled" : {
          "title" : "Use Client-based Sessions",
          "description" : "Enables client-based sessions.<br><br>Client-based sessions provide elastic
 scalability by storing all session state as a JWT in a cookie stored on the client. It is highly
 recommended to enable signing and encryption of the JWT in the global session service.",
          "propertyOrder" : 3800,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "locale" : {
          "title" : "Default Authentication Locale",
          "description" : "",
          "propertyOrder" : 600,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "userStatusCallbackPlugins" : {
          "title" : "Pluggable User Status Event Classes",
          "description" : "List of classes to be called when status of the user account
 changes.<br><br>When the status of a users account changes, OpenAM can be configured to call into
 a custom class. The custom class can then be used to perform some action as required. The built in
 status change events are:<br/><br/><ul><li>Account locked</li><li>Password changed</li></ul><br/
>Custom code can also extend this mechanism.",
```

```
          "propertyOrder" : 2600,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "identityType" : {
          "title" : "Identity Types",
          "description" : "",
          "propertyOrder" : 2500,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "defaultAuthLevel" : {
          "title" : "Default Authentication Level",
          "description" : "The default authentication level for modules in this realm.<br><br>If
the authentication module does not set it's own auth level then the module will have the default
authentication level for the realm.",
          "propertyOrder" : 4100,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "externalLoginPageUrl" : {
          "title" : "External Login Page URL",
          "description" : "Link to the external login user interface.<br><br>If the authentication
user interface is hosted separately from AM, its URL can be provided here. AM will use this
URL for example when it's constructing the resume URI in case authentication is suspended in an
authentication tree.",
          "propertyOrder" : 3910,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "twoFactorRequired" : {
          "title" : "Two Factor Authentication Mandatory",
          "description" : "Enforces ALL 2FA (OATH and Push) authentication Modules (not nodes) only
for this authentication realm.",
          "propertyOrder" : 3900,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        }
      }
    },
    "core" : {
      "type" : "object",
      "title" : "Core",
      "propertyOrder" : -1,
      "properties" : {
        "orgConfig" : {
          "title" : "Organization Authentication Configuration",
```

```
          "description" : "Default Authentication Service for users<br><br>This is the authentication
service that will be used to authenticate users to this realm.",
          "propertyOrder" : 700,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "adminAuthModule" : {
          "title" : "Administrator Authentication Configuration",
          "description" : "Default Authentication Service for administrators<br><br>This is the
authentication service that will be used to authentication administrative users to this realm.",
          "propertyOrder" : 200,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "security" : {
      "type" : "object",
      "title" : "Security",
      "propertyOrder" : 5,
      "properties" : {
        "zeroPageLoginEnabled" : {
          "title" : "Zero Page Login",
          "description" : "Allows a user to authenticate using GET request parameters without
showing the login screen.<br><br>Enable this feature if the authentication mechanism uses a single
authentication screen or the first authentication screen should always be invisible to users (since
it is auto-submitted). Use caution when enabling this feature as it can be used to authenticate using
regular GET parameters, which could be cached by browsers and logged in server and proxy access logs
exposing the values of the GET parameters.",
          "propertyOrder" : 3400,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "moduleBasedAuthEnabled" : {
          "title" : "Module Based Authentication",
          "description" : "Allows a user to authenticate via module based authentication.<br><br>The
feature allow users to override the realm configuration and use a named authentication module to
authenticate.<br/><br/><i>NB </i>Recommended to turn this feature off in production environments.",
          "propertyOrder" : 2800,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "sharedSecret" : {
          "title" : "Organization Authentication Signing Secret",
          "description" : "HMAC shared secret for signing RESTful Authentication requests.<br><br>This
is the shared secret for signing state used in RESTful authentication requests. Should be at Base-64
encoded and at least 128-bits in length. By default a cryptographically secure random value is
generated.",
          "propertyOrder" : 4000,
          "required" : true,
          "type" : "string",
          "format" : "password",
          "exampleValue" : ""
        },
        "zeroPageLoginAllowedWithoutReferrer" : {
```

```
          "title" : "Zero Page Login Allowed without Referer?",
          "description" : "Whether to allow Zero Page Login if the HTTP Referer header is
missing.<br><br>The HTTP Referer header is sometimes missing from requests (e.g., if making a request
to HTTP from HTTPS). This setting controls whether such requests should be allowed or not. Setting
to 'true' will reduce the risk of Login CSRF attacks with Zero Page Login, but may potentially deny
legitimate requests.",
          "propertyOrder" : 3700,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "zeroPageLoginReferrerWhiteList" : {
          "title" : "Zero Page Login Referer Whitelist",
          "description" : "List of allowed HTTP Referer (sic) URLs from which Zero Page Login requests
are allowed.<br><br>Enter here all URLs from which you want to allow Zero Page Login. This provides
some mitigation against Login CSRF attacks. Leave empty to allow from any Referer. Applies to both
GET and POST login requests.",
          "propertyOrder" : 3600,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "keyAlias" : {
          "title" : "Persistent Cookie Encryption Certificate Alias",
          "description" : "Keystore Alias for encrypting Persistent Cookies.<br><br>This is the alias
for the private/public keys in the Keystore used in Persistent Cookie authentication requests.",
          "propertyOrder" : 3300,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "userprofile" : {
      "type" : "object",
      "title" : "User Profile",
      "propertyOrder" : 0,
      "properties" : {
        "aliasAttributeName" : {
          "title" : "Alias Search Attribute Name",
          "description" : "The secondary LDAP attribute retrieves the user profile if the primary
LDAP attribute specified in 'User Naming Attribute' fails.<br><br>This list of LDAP attributes
is used to extend the set of attributes searched by OpenAM to find the users profile.<br>For
example: <ul><li>cn</li><li>mail</li><li>givenname</li></ul><br/>A user authenticates to OpenAM
under the id of steve, OpenAM will first search using the naming attribute (uid by default) so
uid=steve, if no match is found then cn=steve will be searched until a match is found or the list is
exhausted.<br><br/><br/><i>NB </i> Only used when User Profile searching is enabled.",
          "propertyOrder" : 400,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "defaultRole" : {
```

```
          "title" : "User Profile Dynamic Creation Default Roles",
          "description" : "List of roles of which dynamically created users will be a
 member.<br><br>Enter the DN for each role that will be assigned to a new user when their profile has
 been dynamically created by OpenAM.<br/><br/><i>NB </i> Deprecated functionality in OpenAM.",
          "propertyOrder" : 300,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "dynamicProfileCreation" : {
          "title" : "User Profile",
          "description" : "Controls the result of the user profile success post successful
 authentication.<br><br>Controls whether a user profile is required for authentication to be
 successful or if the profile will be dynamically created if none already exists. Choose ignore if you
 do not have a data store configured in the realm.",
          "propertyOrder" : 100,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    }
  }
}
```

Global Operations

Resource path: `/global-config/authentication`

Resource version: `1.0`

read

Usage:

```
am> read Authentication --global
```

update

Usage:

```
am> update Authentication --global --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "ldapConnectionPoolDefaultSize" : {
      "title" : "Default LDAP Connection Pool Size",
      "description" : "The default connection pool size; format is: mininum:maximum",
      "propertyOrder" : 2400,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "authenticators" : {
      "title" : "Pluggable Authentication Module Classes",
      "description" : "List of configured authentication modules<br><br>The list of
 configured authentication modules available to OpenAM. All modules must extend from the
 <code>com.sun.identity.authentication.spi.AMLoginModule</code> class.",
      "propertyOrder" : 500,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "remoteAuthSecurityEnabled" : {
      "title" : "Remote Auth Security",
      "description" : "OpenAM requires authentication client to authenticate itself before
 authenticating users.<br><br>When this setting is enabled, OpenAM will require the authentication
 client (such as a policy agent) to authentication itself to OpenAM before the client will be allow to
 use the remote authentication API to authenticate users. ",
      "propertyOrder" : 2900,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "ldapConnectionPoolSize" : {
      "title" : "LDAP Connection Pool Size",
      "description" : "Controls the size of the LDAP connection pool used for
 authentication<br><br>Control the size of the connection pool to the LDAP directory server used by
 any of the authentication modules that use LDAP directly such as LDAP or Active Directory.Different
 OpenAM servers can be configured with different connection pool settings.<br/><br/>Format:
 host:port:minimum:maximum",
      "propertyOrder" : 2300,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "keepPostProcessInstances" : {
      "title" : "Keep Post Process Objects for Logout Processing",
      "description" : "Store Post Processing Classes for the duration of the session.<br><br>Enabling
 this setting will cause OpenAM to store instances of post processing classes into the users session.
 When the user logs out the original instances of the post processing classes will be called instead
 of new instances. This may be needed for special logout processing.<br/><br/><i>NB </i>Enabling this
 setting will increase the memory usage of OpenAM.",
      "propertyOrder" : 3100,
```

```
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "defaults" : {
      "properties" : {
        "postauthprocess" : {
          "type" : "object",
          "title" : "Post Authentication Processing",
          "propertyOrder" : 6,
          "properties" : {
            "usernameGeneratorClass" : {
              "title" : "Pluggable User Name Generator Class",
              "description" : "The name of the default implementation of the user name
 generator class.<br><br>The name of the class used to return a list of usernames to
 the Membership auth module.<br/><br/><i>NB </i>This class must implement the interface
 <code>com.sun.identity.authentication.spi.UserIDGenerator</code>",
              "propertyOrder" : 2200,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            },
            "loginSuccessUrl" : {
              "title" : "Default Success Login URL",
              "description" : "Successful logins will be forwarded to this URL<br><br>This is the URL
 to which clients will be forwarded upon successful authentication. Enter a URL or URI relative to
 the local OpenAM. URL or URI can be prefixed with the ClientType|URL if client specific. URL without
 http(s) protocol will be appended to the current URI of OpenAM.",
              "propertyOrder" : 1800,
              "required" : true,
              "items" : {
                "type" : "string"
              },
              "type" : "array",
              "exampleValue" : ""
            },
            "loginPostProcessClass" : {
              "title" : "Authentication Post Processing Classes",
              "description" : "A list of post authentication processing classes for all
 users in this realm.<br><br>This is a list of Post Processing Classes that will be called
 by OpenAM for all users that authenticate to this realm. Refer to the documentation for
 the places where the list of post authentication classes can be set and their precedence.
 <br/><br/>For example: org.forgerock.auth.PostProcessClass<br/><i>NB </i>OpenAM must be
 able to find these classes on the <code>CLASSPATH</code> and must implement the interface
 <code>com.sun.identity.authentication.spi.AMPostAuthProcessInterface</code>.",
              "propertyOrder" : 2000,
              "required" : true,
              "items" : {
                "type" : "string"
              },
              "type" : "array",
              "exampleValue" : ""
            },
            "userAttributeSessionMapping" : {
              "title" : "User Attribute Mapping to Session Attribute",
              "description" : "Mapping of user profile attribute name to session attribute
 name.<br><br>The setting causes OpenAM to read the named attributes from the users profile in the
 data store and store their values in the users session.<br/></br>Format: User Profile Attribute|
Session Attribute name. ",
```

```
              "propertyOrder" : 3000,
              "required" : true,
              "items" : {
                "type" : "string"
              },
              "type" : "array",
              "exampleValue" : ""
            },
            "usernameGeneratorEnabled" : {
              "title" : "Generate UserID Mode",
              "description" : "Enables this mode in the Membership auth module.<br><br>When this mode
is enabled, if the Membership auth module detects that the supplied username already exists in the
data store then a list of valid usernames can be shown to the user, if requested by said user.",
              "propertyOrder" : 2100,
              "required" : true,
              "type" : "boolean",
              "exampleValue" : ""
            },
            "loginFailureUrl" : {
              "title" : "Default Failure Login URL ",
              "description" : "Failed logins will be forwarded to this URL<br><br>This is the URL
to which clients will be forwarded upon failed authentication. Enter a URL or URI relative to the
local OpenAM. URL or URI can be prefixed with ClientType|URL if client specific. URL without http(s)
protocol will be appended to the current URI of OpenAM.",
              "propertyOrder" : 1900,
              "required" : true,
              "items" : {
                "type" : "string"
              },
              "type" : "array",
              "exampleValue" : ""
            }
          }
        },
        "accountlockout" : {
          "type" : "object",
          "title" : "Account Lockout",
          "propertyOrder" : 2,
          "properties" : {
            "lockoutAttributeName" : {
              "title" : "Lockout Attribute Name",
              "description" : "Name of custom lockout attribute <br><br>When OpenAM locks an account,
the <code>inetuserstatus</code> attribute in the locked account is set to Inactive. In addition,
OpenAM can set the value of another attribute in the users profile. ",
              "propertyOrder" : 1500,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            },
            "lockoutDuration" : {
              "title" : "Login Failure Lockout Duration",
              "description" : "The duration of the users account lockout, in minutes.<br><br>OpenAM
can either lockout the users account indefinitely (until administration action) by setting the
duration to 0, (the default) or OpenAM can lock the users account for a given number of minutes.
After the lockout interval, the user will be able to successfully authenticate to OpenAM.",
              "propertyOrder" : 1300,
              "required" : true,
              "type" : "integer",
              "exampleValue" : ""
```

```
            },
            "lockoutWarnUserCount" : {
              "title" : "Warn User After N Failures",
              "description" : "Warn the user when they reach this level of failed
authentications.<br><br>The user will be given a warning when they reach this level of failed
authentications during the lockout interval.<br/>The text of the lockout warning is configured using
the <code>lockOutWarning</code> property in the <code>amAuth.properties</code> file.",
              "propertyOrder" : 1200,
              "required" : true,
              "type" : "integer",
              "exampleValue" : ""
            },
            "invalidAttemptsDataAttributeName" : {
              "title" : "Invalid Attempts Data Attribute Name",
              "description" : "The name of the attribute used to store information about failed
authentications.<br><br>OpenAM can be configured to store information about invalid authentications
in the users profile. This allows multiple instances of OpenAM in the same site to share
information about a users invalid authentication attempts. By default the custom attribute;
<code>sunAMAuthInvalidAttemptsData</code> defined in the <code>sunAMAuthAccountLockout</code>
objectclass is used to store this data. Use this property to change the attribute used by OpenAM to
store this information.<br/><br/><i>NB </i>Any attribute specified must be a valid attribute in the
data store.",
              "propertyOrder" : 1700,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            },
            "lockoutDurationMultiplier" : {
              "title" : "Lockout Duration Multiplier",
              "description" : "Value multiplied to the Login Failure Lockout Duration for each
successive lockout.<br><br>This property is used to enable OpenAM to increase the account lockout
duration for each successive account lockout. For example: If the lockout duration is set to 10 and
the duration multiplier is set to 2; the duration of the first lockout will be 10 minutes and the
duration of the second lockout will be 20 minutes.<br/><br/>The default value of 1 disables this
function.  ",
              "propertyOrder" : 1400,
              "required" : true,
              "type" : "integer",
              "exampleValue" : ""
            },
            "loginFailureDuration" : {
              "title" : "Login Failure Lockout Interval",
              "description" : "The lockout interval time is in minutes.<br><br>OpenAM tracks the
failed authentication count for a user over the lockout interval.<br/><br/>For example: If the
lockout interval is 5 minutes and the lockout count is 5; the user will have to have failed to
authenticate 5 times over the previous 5 minutes for the account to be locked. Failed authentications
the occurred outside of the 5 minute interval are ignored.",
              "propertyOrder" : 1000,
              "required" : true,
              "type" : "integer",
              "exampleValue" : ""
            },
            "lockoutAttributeValue" : {
              "title" : "Lockout Attribute Value",
              "description" : "Value to set in custom lockout attribute<br><br>This is the value that
will be set on the custom attribute in the users profile when they account is locked.",
              "propertyOrder" : 1600,
              "required" : true,
              "type" : "string",
```

```
              "exampleValue" : ""
            },
            "loginFailureCount" : {
              "title" : "Login Failure Lockout Count",
              "description" : "The maximum number of failed authentications for a user before their
 account is locked.<br><br>This setting controls the maximum number of failed authentications a user
 can have during the lockout interval before OpenAM locks the users account.",
              "propertyOrder" : 900,
              "required" : true,
              "type" : "integer",
              "exampleValue" : ""
            },
            "storeInvalidAttemptsInDataStore" : {
              "title" : "Store Invalid Attempts in Data Store",
              "description" : "Enables sharing of login failure attempts across AM
 Instances<br><br>When this setting is enabled AM will store the user's invalid authentication
 information in the data store under the attribute configured in the <i>Invalid Attempts Data
 Attribute Name</i> property. This setting only applies to authentication modules and chains;
 authentication trees will <i>always</i> write their account lockout progress and status to the data
 store.",
              "propertyOrder" : 2700,
              "required" : true,
              "type" : "boolean",
              "exampleValue" : ""
            },
            "loginFailureLockoutMode" : {
              "title" : "Login Failure Lockout Mode",
              "description" : "Enables account lockout functionality for users authenticating to this
 realm.<br><br>OpenAM can track the number of failed authentications by a user over time and if a pre-
defined limit is breached, OpenAM can lockout the users account and perform additional functions.<br/
><br/><i>NB </i>This functionality is in addition to any account lockout behaviour implemented by the
 LDAP Directory Server.",
              "propertyOrder" : 800,
              "required" : true,
              "type" : "boolean",
              "exampleValue" : ""
            },
            "lockoutEmailAddress" : {
              "title" : "Email Address to Send Lockout Notification",
              "description" : "An email address or set of email addresses that receive notifications
 about account lockout events.<br><br>OpenAM can be configured to send a localisable email
 message to a set of email addresses when account lockout events occur. The contents of the
 email message is configured using the following properties in the <code>amAuth.properties</code>
 file.<br/><ul><li><code>lockOutEmailFrom</code> : The \"From\" address of the email message</
li><li><code>lockOutEmailSub</code> : The subject of the email message</li><li><code>lockOutEmailMsg</
code> : The contents of the email message</li></ul><br/>The identity for whom the account has
 been locked is included in the email message.<br/><br/>The format of this property is:<br/
><code>emailaddress|locale|charset</code>. Multiple email addresses are space-separated.<br/>Email
 addresses must include the domain name, such as <code>admin@example.com</code>.",
              "propertyOrder" : 1100,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            }
          }
        },
        "trees" : {
          "type" : "object",
          "title" : "Trees",
```

```
          "propertyOrder" : 4,
          "properties" : {
            "authenticationSessionsMaxDuration" : {
              "title" : "Max duration (minutes)",
              "description" : "Specify how long an authentication session can last.<br><br>From
 the time an authentication session is generated, the session will be invalid after this number of
 minutes. Values from <strong>1</strong> upwards are allowed.",
              "propertyOrder" : 3860,
              "required" : true,
              "type" : "integer",
              "exampleValue" : ""
            },
            "authenticationSessionsWhitelist" : {
              "title" : "Enable whitelisting",
              "description" : "Enables explicit whitelisting of valid authentication states to prevent
 replay attacks.<br><br>If enabled, each time a response is sent to the user a randomly generated
 state parameter is also sent back to user. This state parameter is stored accessible to AM and
 must be sent in with the subsequent request. After a request has been received with a valid state
 parameter, the next response contains a new state, and the server's view of the valid state parameter
 is updated.",
              "propertyOrder" : 3880,
              "required" : true,
              "type" : "boolean",
              "exampleValue" : ""
            },
            "suspendedAuthenticationTimeout" : {
              "title" : "Suspended authentication duration (minutes)",
              "description" : "Specify how long a suspended authentication session can
 last.<br><br>From the time a suspended authentication session is generated, the session will be
 invalid after this number of minutes. Values from <strong>1</strong> upwards are allowed. This
 timeout should be less than or equal to the authentication sessionâ##s timeout value.",
              "propertyOrder" : 3870,
              "required" : true,
              "type" : "integer",
              "exampleValue" : ""
            },
            "authenticationSessionsStateManagement" : {
              "title" : "Authentication session state management scheme",
              "description" : "Specify how the authentication session state is managed.<br><br>CTS
 option will write the state down to the underlying core token store.<br />JWT option will transmit
 the state in a JWT to the client.<br />In-Memory option will maintain the state in the memory
 (requires sticky loadbalancing).<br /><br /> <em>To configure JWT signing, encryption, and
 blacklisting use the options in the Client-based Sessions section of the Sessions global service.</
em>",
              "propertyOrder" : 3850,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            }
          }
        },
        "general" : {
          "type" : "object",
          "title" : "General",
          "propertyOrder" : 3,
          "properties" : {
            "locale" : {
              "title" : "Default Authentication Locale",
              "description" : "",
```

```
              "propertyOrder" : 600,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            },
            "statelessSessionsEnabled" : {
              "title" : "Use Client-based Sessions",
              "description" : "Enables client-based sessions.<br><br>Client-based sessions provide
 elastic scalability by storing all session state as a JWT in a cookie stored on the client. It is
 highly recommended to enable signing and encryption of the JWT in the global session service.",
              "propertyOrder" : 3800,
              "required" : true,
              "type" : "boolean",
              "exampleValue" : ""
            },
            "externalLoginPageUrl" : {
              "title" : "External Login Page URL",
              "description" : "Link to the external login user interface.<br><br>If the authentication
 user interface is hosted separately from AM, its URL can be provided here. AM will use this
 URL for example when it's constructing the resume URI in case authentication is suspended in an
 authentication tree.",
              "propertyOrder" : 3910,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            },
            "defaultAuthLevel" : {
              "title" : "Default Authentication Level",
              "description" : "The default authentication level for modules in this realm.<br><br>If
 the authentication module does not set it's own auth level then the module will have the default
 authentication level for the realm.",
              "propertyOrder" : 4100,
              "required" : true,
              "type" : "integer",
              "exampleValue" : ""
            },
            "twoFactorRequired" : {
              "title" : "Two Factor Authentication Mandatory",
              "description" : "Enforces ALL 2FA (OATH and Push) authentication Modules (not nodes)
 only for this authentication realm.",
              "propertyOrder" : 3900,
              "required" : true,
              "type" : "boolean",
              "exampleValue" : ""
            },
            "userStatusCallbackPlugins" : {
              "title" : "Pluggable User Status Event Classes",
              "description" : "List of classes to be called when status of the user account
 changes.<br><br>When the status of a users account changes, OpenAM can be configured to call into
 a custom class. The custom class can then be used to perform some action as required. The built in
 status change events are:<br/><br/><ul><li>Account locked</li><li>Password changed</li></ul><br/
>Custom code can also extend this mechanism.",
              "propertyOrder" : 2600,
              "required" : true,
              "items" : {
                "type" : "string"
              },
              "type" : "array",
              "exampleValue" : ""
```

```
            },
            "identityType" : {
              "title" : "Identity Types",
              "description" : "",
              "propertyOrder" : 2500,
              "required" : true,
              "items" : {
                "type" : "string"
              },
              "type" : "array",
              "exampleValue" : ""
            }
          }
        },
        "userprofile" : {
          "type" : "object",
          "title" : "User Profile",
          "propertyOrder" : 0,
          "properties" : {
            "dynamicProfileCreation" : {
              "title" : "User Profile",
              "description" : "Controls the result of the user profile success post successful
authentication.<br><br>Controls whether a user profile is required for authentication to be
successful or if the profile will be dynamically created if none already exists. Choose ignore if you
do not have a data store configured in the realm.",
              "propertyOrder" : 100,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            },
            "defaultRole" : {
              "title" : "User Profile Dynamic Creation Default Roles",
              "description" : "List of roles of which dynamically created users will be a
member.<br><br>Enter the DN for each role that will be assigned to a new user when their profile has
been dynamically created by OpenAM.<br/><br/><i>NB </i> Deprecated functionality in OpenAM.",
              "propertyOrder" : 300,
              "required" : true,
              "items" : {
                "type" : "string"
              },
              "type" : "array",
              "exampleValue" : ""
            },
            "aliasAttributeName" : {
              "title" : "Alias Search Attribute Name",
              "description" : "The secondary LDAP attribute retrieves the user profile if the primary
LDAP attribute specified in 'User Naming Attribute' fails.<br><br>This list of LDAP attributes
is used to extend the set of attributes searched by OpenAM to find the users profile.<br>For
example: <ul><li>cn</li><li>mail</li><li>givenname</li></ul><br/>A user authenticates to OpenAM
under the id of steve, OpenAM will first search using the naming attribute (uid by default) so
uid=steve, if no match is found then cn=steve will be searched until a match is found or the list is
exhausted.<br><br/><br/><i>NB </i> Only used when User Profile searching is enabled.",
              "propertyOrder" : 400,
              "required" : true,
              "items" : {
                "type" : "string"
              },
              "type" : "array",
              "exampleValue" : ""
```

```
          }
        }
      },
      "security" : {
        "type" : "object",
        "title" : "Security",
        "propertyOrder" : 5,
        "properties" : {
          "zeroPageLoginReferrerWhiteList" : {
            "title" : "Zero Page Login Referer Whitelist",
            "description" : "List of allowed HTTP Referer (sic) URLs from which Zero Page Login
requests are allowed.<br><br>Enter here all URLs from which you want to allow Zero Page Login. This
provides some mitigation against Login CSRF attacks. Leave empty to allow from any Referer. Applies
to both GET and POST login requests.",
            "propertyOrder" : 3600,
            "required" : true,
            "items" : {
              "type" : "string"
            },
            "type" : "array",
            "exampleValue" : ""
          },
          "sharedSecret" : {
            "title" : "Organization Authentication Signing Secret",
            "description" : "HMAC shared secret for signing RESTful Authentication
requests.<br><br>This is the shared secret for signing state used in RESTful authentication requests.
Should be at Base-64 encoded and at least 128-bits in length. By default a cryptographically secure
random value is generated.",
            "propertyOrder" : 4000,
            "required" : true,
            "type" : "string",
            "format" : "password",
            "exampleValue" : ""
          },
          "moduleBasedAuthEnabled" : {
            "title" : "Module Based Authentication",
            "description" : "Allows a user to authenticate via module based
authentication.<br><br>The feature allow users to override the realm configuration and use a named
authentication module to authenticate.<br/><br/><i>NB </i>Recommended to turn this feature off in
production environments.",
            "propertyOrder" : 2800,
            "required" : true,
            "type" : "boolean",
            "exampleValue" : ""
          },
          "zeroPageLoginEnabled" : {
            "title" : "Zero Page Login",
            "description" : "Allows a user to authenticate using GET request parameters without
showing the login screen.<br><br>Enable this feature if the authentication mechanism uses a single
authentication screen or the first authentication screen should always be invisible to users (since
it is auto-submitted). Use caution when enabling this feature as it can be used to authenticate using
regular GET parameters, which could be cached by browsers and logged in server and proxy access logs
exposing the values of the GET parameters.",
            "propertyOrder" : 3400,
            "required" : true,
            "type" : "boolean",
            "exampleValue" : ""
          },
          "keyAlias" : {
```

```
              "title" : "Persistent Cookie Encryption Certificate Alias",
              "description" : "Keystore Alias for encrypting Persistent Cookies.<br><br>This is
 the alias for the private/public keys in the Keystore used in Persistent Cookie authentication
 requests.",
              "propertyOrder" : 3300,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            },
            "zeroPageLoginAllowedWithoutReferrer" : {
              "title" : "Zero Page Login Allowed without Referer?",
              "description" : "Whether to allow Zero Page Login if the HTTP Referer header is
 missing.<br><br>The HTTP Referer header is sometimes missing from requests (e.g., if making a request
 to HTTP from HTTPS). This setting controls whether such requests should be allowed or not. Setting
 to 'true' will reduce the risk of Login CSRF attacks with Zero Page Login, but may potentially deny
 legitimate requests.",
              "propertyOrder" : 3700,
              "required" : true,
              "type" : "boolean",
              "exampleValue" : ""
            }
          }
        },
        "core" : {
          "type" : "object",
          "title" : "Core",
          "propertyOrder" : -1,
          "properties" : {
            "orgConfig" : {
              "title" : "Organization Authentication Configuration",
              "description" : "Default Authentication Service for users<br><br>This is the
 authentication service that will be used to authenticate users to this realm.",
              "propertyOrder" : 700,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            },
            "adminAuthModule" : {
              "title" : "Administrator Authentication Configuration",
              "description" : "Default Authentication Service for administrators<br><br>This is the
 authentication service that will be used to authentication administrative users to this realm.",
              "propertyOrder" : 200,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            }
          }
        }
      },
      "type" : "object",
      "title" : "Realm Defaults"
    }
  }
}
```

AuthenticationChains

Realm Operations

Resource path: `/realm-config/authentication/chains`

Resource version: `1.0`

create

Usage:

```
am> create AuthenticationChains --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "loginPostProcessClass" : {
      "title" : "Authentication Post Processing Classes",
      "description" : "Example: com.abc.authentication.PostProcessClass",
      "propertyOrder" : 400,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "authChainConfiguration" : {
      "title" : "Authentication Configuration",
      "description" : "",
      "propertyOrder" : 100,
      "required" : true,
      "exampleValue" : "",
      "type" : "array",
      "items" : {
        "type" : "object",
        "properties" : {
          "module" : {
            "type" : "string"
          },
          "criteria" : {
            "type" : "string"
```

```
          },
          "options" : {
            "type" : "object",
            "patternProperties" : {
              ".*" : {
                "type" : "string"
              }
            }
          }
        }
      }
    },
    "loginFailureUrl" : {
      "title" : "Login Failed URL",
      "description" : "URL or ClientType|URL if client specific. URL without http(s) protocol will be
 appended to the current URI.",
      "propertyOrder" : 300,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "loginSuccessUrl" : {
      "title" : "Login Success URL",
      "description" : "URL or ClientType|URL if client specific. URL without http(s) protocol will be
 appended to the current URI.",
      "propertyOrder" : 200,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    }
  }
}
```

delete

Usage:

```
am> delete AuthenticationChains --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action AuthenticationChains --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action AuthenticationChains --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action AuthenticationChains --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query AuthenticationChains --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read AuthenticationChains --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update AuthenticationChains --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "loginPostProcessClass" : {
      "title" : "Authentication Post Processing Classes",
      "description" : "Example: com.abc.authentication.PostProcessClass",
      "propertyOrder" : 400,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "authChainConfiguration" : {
      "title" : "Authentication Configuration",
      "description" : "",
      "propertyOrder" : 100,
      "required" : true,
      "exampleValue" : "",
      "type" : "array",
      "items" : {
        "type" : "object",
        "properties" : {
          "module" : {
            "type" : "string"
          },
          "criteria" : {
            "type" : "string"
          },
          "options" : {
            "type" : "object",
            "patternProperties" : {
              ".*" : {
                "type" : "string"
              }
            }
          }
        }
      }
    },
    "loginFailureUrl" : {
      "title" : "Login Failed URL",
```

```
      "description" : "URL or ClientType|URL if client specific. URL without http(s) protocol will be
 appended to the current URI.",
      "propertyOrder" : 300,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "loginSuccessUrl" : {
      "title" : "Login Success URL",
      "description" : "URL or ClientType|URL if client specific. URL without http(s) protocol will be
 appended to the current URI.",
      "propertyOrder" : 200,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    }
  }
}
```

Global Operations

Resource path: `/global-config/authentication/chains`

Resource version: `1.0`

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action AuthenticationChains --global --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action AuthenticationChains --global --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action AuthenticationChains --global --actionName nextdescendents
```

read

Usage:

```
am> read AuthenticationChains --global
```

update

Usage:

```
am> update AuthenticationChains --global --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "dynamic" : {
      "properties" : {
        "authChainConfiguration" : {
          "title" : "Authentication Configuration",
          "description" : "",
          "propertyOrder" : 100,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      },
      "type" : "object",
      "title" : "Dynamic Attributes"
    }
  }
}
```

AuthenticationModules

Realm Operations

The collection of all authentication modules in a realm allows querying for all module instances.

Resource path: `/realm-config/authentication/modules`

Resource version: `1.0`

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action AuthenticationModules --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action AuthenticationModules --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action AuthenticationModules --realm Realm --actionName nextdescendents
```

query

Query for authentication module instances

Usage:

```
am> query AuthenticationModules --realm Realm --filter filter
```

Parameters:

`--filter`

A CREST formatted query filter, where "true" will query all. Fields that can be queried: [_id]

Global Operations

Global and default configuration for authentication modules

Resource path: `/global-config/authentication/modules`

Resource version: `1.0`

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action AuthenticationModules --global --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action AuthenticationModules --global --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action AuthenticationModules --global --actionName nextdescendents
```

AuthenticationNodes

Realm Operations

Auth Tree Nodes

Resource path: `/realm-config/authentication/authenticationtrees/nodes`

Resource version: `1.0`

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action AuthenticationNodes --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action AuthenticationNodes --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action AuthenticationNodes --realm Realm --actionName nextdescendents
```

AuthenticationTreesConfiguration

Realm Operations

Sub-path parent for all authentication tree configuration.

Resource path: `/realm-config/authentication/authenticationtrees`

Resource version: `1.0`

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action AuthenticationTreesConfiguration --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action AuthenticationTreesConfiguration --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action AuthenticationTreesConfiguration --realm Realm --actionName nextdescendents
```

Global Operations

Resource path: `/global-config/authentication/authenticationtrees`

Resource version: `1.0`

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action AuthenticationTreesConfiguration --global --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action AuthenticationTreesConfiguration --global --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action AuthenticationTreesConfiguration --global --actionName nextdescendents
```

read

Usage:

```
am> read AuthenticationTreesConfiguration --global
```

update

Usage:

```
am> update AuthenticationTreesConfiguration --global --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object"
}
```

AuthenticatorOath

Realm Operations

Resource path: `/realm-config/services/authenticatorOathService`

Resource version: `1.0`

create

Usage:

```
am> create AuthenticatorOath --realm Realm --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "authenticatorOATHDeviceSettingsEncryptionKeystorePrivateKeyPassword" : {
      "title" : "Private Key Password",
      "description" : "Password to unlock the private key.",
      "propertyOrder" : 700,
      "required" : true,
      "type" : "string",
      "format" : "password",
      "exampleValue" : ""
    },
    "authenticatorOATHDeviceSettingsEncryptionKeystoreType" : {
      "title" : "Key Store Type",
      "description" : "Type of encryption key store.<br><br><i>Note:</i> PKCS#11 keys tores require
 hardware support such as a security device or smart card and is not available by default in most
 JVM installations.<p><p>See the <a href=\"https://docs.oracle.com/javase/8/docs/technotes/guides/
security/p11guide.html\" target=\"_blank\">JDK 8 PKCS#11 Reference Guide</a> for more details.",
      "propertyOrder" : 400,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "authenticatorOATHSkippableName" : {
      "title" : "ForgeRock Authenticator (OATH) Device Skippable Attribute Name",
      "description" : "The data store attribute that holds the user's decision to enable or disable
 obtaining and providing a password obtained from the ForgeRock Authenticator app. This attribute must
 be writeable.",
      "propertyOrder" : 800,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
```

```
    },
    "authenticatorOATHDeviceSettingsEncryptionScheme" : {
      "title" : "Device Profile Encryption Scheme",
      "description" : "Encryption scheme for securing device profiles stored on the server.<br><br>If
 enabled, each device profile is encrypted using a unique random secret key using the given strength
 of AES encryption in CBC mode with PKCS#5 padding. An HMAC-SHA of the given strength (truncated to
 half-size) is used to ensure integrity protection and authenticated encryption. The unique random
 key is encrypted with the given RSA key pair and stored with the device profile.<p><p><i>Note:</i>
 AES-256 may require installation of the JCE Unlimited Strength policy files.",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "authenticatorOATHDeviceSettingsEncryptionKeystore" : {
      "title" : "Encryption Key Store",
      "description" : "Path to the key store from which to load encryption keys.",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "authenticatorOATHDeviceSettingsEncryptionKeystorePassword" : {
      "title" : "Key Store Password",
      "description" : "Password to unlock the key store. This password will be encrypted.",
      "propertyOrder" : 500,
      "required" : true,
      "type" : "string",
      "format" : "password",
      "exampleValue" : ""
    },
    "oathAttrName" : {
      "title" : "Profile Storage Attribute",
      "description" : "Attribute for storing ForgeRock Authenticator OATH profiles.<br><br>The default
 attribute is added to the user store during OpenAM installation. If you want to use a different
 attribute, you must make sure to add it to your user store schema prior to deploying two-step
 verification with a ForgeRock OATH authenticator app in OpenAM. OpenAM must be able to write to the
 attribute.",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "authenticatorOATHDeviceSettingsEncryptionKeystoreKeyPairAlias" : {
      "title" : "Key-Pair Alias",
      "description" : "Alias of the certificate and private key in the key store. The private key is
 used to encrypt and decrypt device profiles.",
      "propertyOrder" : 600,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
```

delete

Usage:

```
am> delete AuthenticatorOath --realm Realm
```

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action AuthenticatorOath --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action AuthenticatorOath --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action AuthenticatorOath --realm Realm --actionName nextdescendents
```

read

Usage:

```
am> read AuthenticatorOath --realm Realm
```

update

Usage:

```
am> update AuthenticatorOath --realm Realm --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "authenticatorOATHDeviceSettingsEncryptionKeystorePrivateKeyPassword" : {
      "title" : "Private Key Password",
```

```
      "description" : "Password to unlock the private key.",
      "propertyOrder" : 700,
      "required" : true,
      "type" : "string",
      "format" : "password",
      "exampleValue" : ""
    },
    "authenticatorOATHDeviceSettingsEncryptionKeystoreType" : {
      "title" : "Key Store Type",
      "description" : "Type of encryption key store.<br><br><i>Note:</i> PKCS#11 keys tores require
 hardware support such as a security device or smart card and is not available by default in most
 JVM installations.<p><p>See the <a href=\"https://docs.oracle.com/javase/8/docs/technotes/guides/
security/p11guide.html\" target=\"_blank\">JDK 8 PKCS#11 Reference Guide</a> for more details.",
      "propertyOrder" : 400,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "authenticatorOATHSkippableName" : {
      "title" : "ForgeRock Authenticator (OATH) Device Skippable Attribute Name",
      "description" : "The data store attribute that holds the user's decision to enable or disable
 obtaining and providing a password obtained from the ForgeRock Authenticator app. This attribute must
 be writeable.",
      "propertyOrder" : 800,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "authenticatorOATHDeviceSettingsEncryptionScheme" : {
      "title" : "Device Profile Encryption Scheme",
      "description" : "Encryption scheme for securing device profiles stored on the server.<br><br>If
 enabled, each device profile is encrypted using a unique random secret key using the given strength
 of AES encryption in CBC mode with PKCS#5 padding. An HMAC-SHA of the given strength (truncated to
 half-size) is used to ensure integrity protection and authenticated encryption. The unique random
 key is encrypted with the given RSA key pair and stored with the device profile.<p><p><i>Note:</i>
 AES-256 may require installation of the JCE Unlimited Strength policy files.",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "authenticatorOATHDeviceSettingsEncryptionKeystore" : {
      "title" : "Encryption Key Store",
      "description" : "Path to the key store from which to load encryption keys.",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "authenticatorOATHDeviceSettingsEncryptionKeystorePassword" : {
      "title" : "Key Store Password",
      "description" : "Password to unlock the key store. This password will be encrypted.",
      "propertyOrder" : 500,
      "required" : true,
      "type" : "string",
      "format" : "password",
      "exampleValue" : ""
    },
    "oathAttrName" : {
```

```
      "title" : "Profile Storage Attribute",
      "description" : "Attribute for storing ForgeRock Authenticator OATH profiles.<br><br>The default
 attribute is added to the user store during OpenAM installation. If you want to use a different
 attribute, you must make sure to add it to your user store schema prior to deploying two-step
 verification with a ForgeRock OATH authenticator app in OpenAM. OpenAM must be able to write to the
 attribute.",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "authenticatorOATHDeviceSettingsEncryptionKeystoreKeyPairAlias" : {
      "title" : "Key-Pair Alias",
      "description" : "Alias of the certificate and private key in the key store. The private key is
 used to encrypt and decrypt device profiles.",
      "propertyOrder" : 600,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
```

Global Operations

Resource path: `/global-config/services/authenticatorOathService`

Resource version: `1.0`

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action AuthenticatorOath --global --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action AuthenticatorOath --global --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action AuthenticatorOath --global --actionName nextdescendents
```

read

Usage:

```
am> read AuthenticatorOath --global
```

update

Usage:

```
am> update AuthenticatorOath --global --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "defaults" : {
      "properties" : {
        "authenticatorOATHSkippableName" : {
          "title" : "ForgeRock Authenticator (OATH) Device Skippable Attribute Name",
          "description" : "The data store attribute that holds the user's decision to enable or
 disable obtaining and providing a password obtained from the ForgeRock Authenticator app. This
 attribute must be writeable.",
          "propertyOrder" : 800,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "authenticatorOATHDeviceSettingsEncryptionKeystorePrivateKeyPassword" : {
          "title" : "Private Key Password",
          "description" : "Password to unlock the private key.",
          "propertyOrder" : 700,
          "required" : true,
          "type" : "string",
          "format" : "password",
          "exampleValue" : ""
        },
        "authenticatorOATHDeviceSettingsEncryptionKeystore" : {
          "title" : "Encryption Key Store",
          "description" : "Path to the key store from which to load encryption keys.",
          "propertyOrder" : 300,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "authenticatorOATHDeviceSettingsEncryptionKeystoreType" : {
          "title" : "Key Store Type",
          "description" : "Type of encryption key store.<br><br><i>Note:</i> PKCS#11 keys tores
 require hardware support such as a security device or smart card and is not available by default
 in most JVM installations.<p><p>See the <a href=\"https://docs.oracle.com/javase/8/docs/technotes/
```

```
guides/security/p11guide.html\" target=\"_blank\">JDK 8 PKCS#11 Reference Guide</a> for more
 details.",
          "propertyOrder" : 400,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "oathAttrName" : {
          "title" : "Profile Storage Attribute",
          "description" : "Attribute for storing ForgeRock Authenticator OATH profiles.<br><br>The
 default attribute is added to the user store during OpenAM installation. If you want to use a
 different attribute, you must make sure to add it to your user store schema prior to deploying two-
step verification with a ForgeRock OATH authenticator app in OpenAM. OpenAM must be able to write to
 the attribute.",
          "propertyOrder" : 100,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "authenticatorOATHDeviceSettingsEncryptionKeystorePassword" : {
          "title" : "Key Store Password",
          "description" : "Password to unlock the key store. This password will be encrypted.",
          "propertyOrder" : 500,
          "required" : true,
          "type" : "string",
          "format" : "password",
          "exampleValue" : ""
        },
        "authenticatorOATHDeviceSettingsEncryptionKeystoreKeyPairAlias" : {
          "title" : "Key-Pair Alias",
          "description" : "Alias of the certificate and private key in the key store. The private key
 is used to encrypt and decrypt device profiles.",
          "propertyOrder" : 600,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "authenticatorOATHDeviceSettingsEncryptionScheme" : {
          "title" : "Device Profile Encryption Scheme",
          "description" : "Encryption scheme for securing device profiles stored on the
 server.<br><br>If enabled, each device profile is encrypted using a unique random secret key
 using the given strength of AES encryption in CBC mode with PKCS#5 padding. An HMAC-SHA of the
 given strength (truncated to half-size) is used to ensure integrity protection and authenticated
 encryption. The unique random key is encrypted with the given RSA key pair and stored with the device
 profile.<p><p><i>Note:</i> AES-256 may require installation of the JCE Unlimited Strength policy
 files.",
          "propertyOrder" : 200,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      },
      "type" : "object",
      "title" : "Realm Defaults"
    }
  }
}
```

AuthenticatorOathModule

Realm Operations

Resource path: `/realm-config/authentication/modules/authenticatoroath`

Resource version: `1.0`

create

Usage:

```
am> create AuthenticatorOathModule --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "minimumSecretKeyLength" : {
      "title" : "Minimum Secret Key Length",
      "description" : "Number of hexadecimal characters allowed for the Secret Key.",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "addChecksumToOtpEnabled" : {
      "title" : "Add Checksum Digit",
      "description" : "This adds a checksum digit to the OTP.<br><br>This adds a digit to the end
 of the OTP generated to be used as a checksum to verify the OTP was generated correctly. This is in
 addition to the actual password length. You should only set this if your device supports it.",
      "propertyOrder" : 600,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "oathAlgorithm" : {
      "title" : "OATH Algorithm to Use",
      "description" : "Choose the algorithm your device uses to generate the OTP.<br><br>HOTP uses a
 counter value that is incremented every time a new OTP is generated. TOTP generates a new OTP every
 few seconds as specified by the time step interval.",
      "propertyOrder" : 400,
      "required" : true,
      "type" : "string",
```

```
      "exampleValue" : ""
    },
    "oathIssuerName" : {
      "title" : "Name of the Issuer",
      "description" : "Name to identify the OTP issuer.",
      "propertyOrder" : 1100,
      "required" : true,
      "type" : "string",
      "exampleValue" : "ForgeRock"
    },
    "totpMaximumClockDrift" : {
      "title" : "Maximum Allowed Clock Drift",
      "description" : "Number of time steps a client is allowed to get out of sync with the server
before manual resynchronisation is required. For example, with 3 allowed drifts and a time step
interval of 30 seconds the server will allow codes from up to 90 seconds from the current time to be
treated as the current time step. The drift for a user's device is calculated each time they enter a
new code. If the drift exceeds this value, the user's authentication code will be rejected.",
      "propertyOrder" : 1000,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "hotpWindowSize" : {
      "title" : "HOTP Window Size",
      "description" : "The size of the window to resynchronize with the client.<br><br>This sets the
window that the OTP device and the server counter can be out of sync. For example, if the window size
is 100 and the servers last successful login was at counter value 2, then the server will accept a
OTP from the OTP device that is from device counter 3 to 102.",
      "propertyOrder" : 500,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "truncationOffset" : {
      "title" : "Truncation Offset",
      "description" : "This adds an offset to the generation of the OTP.<br><br>This is an option used
by the HOTP algorithm that not all devices support. This should be left default unless you know your
device uses a offset.",
      "propertyOrder" : 700,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "authenticationLevel" : {
      "title" : "Authentication Level",
      "description" : "The authentication level associated with this module.<br><br>Each
authentication module has an authentication level that can be used to indicate the level of security
associated with the module; 0 is the lowest (and the default).",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "totpTimeStepInterval" : {
      "title" : "TOTP Time Step Interval",
      "description" : "The TOTP time step in seconds that the OTP device uses to generate the
OTP.<br><br>This is the time interval that one OTP is valid for. For example, if the time step is 30
seconds, then a new OTP will be generated every 30 seconds. This makes a single OTP valid for only 30
seconds.",
```

```
      "propertyOrder" : 800,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "frOathOtpMaxRetry" : {
      "title" : "One Time Password Max Retry",
      "description" : "The number of times entry of the OTP may be attempted. Minimum is 1 maximum is
 10 and default is 3.",
      "propertyOrder" : null,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "passwordLength" : {
      "title" : "One Time Password Length ",
      "description" : "The length of the generated OTP in digits, must be at least 6 and compatible
 with the hardware/software OTP generators you expect your end-users to use. For example, Google and
 ForgeRock authenticators support values of 6 and 8.",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "totpTimeStepsInWindow" : {
      "title" : "TOTP Time Steps",
      "description" : "The number of time steps to check before and after receiving a OTP.<br><br>This
 is the number of time step intervals to check the received OTP against both forward in time and back
 in time. For example, with 1 time steps and a time step interval of 30 seconds the server will allow
 a code between the previous code, the current code and the next code.",
      "propertyOrder" : 900,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    }
  }
}
```

delete

Usage:

```
am> delete AuthenticatorOathModule --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action AuthenticatorOathModule --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action AuthenticatorOathModule --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action AuthenticatorOathModule --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query AuthenticatorOathModule --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read AuthenticatorOathModule --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update AuthenticatorOathModule --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "minimumSecretKeyLength" : {
      "title" : "Minimum Secret Key Length",
      "description" : "Number of hexadecimal characters allowed for the Secret Key.",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "addChecksumToOtpEnabled" : {
      "title" : "Add Checksum Digit",
      "description" : "This adds a checksum digit to the OTP.<br><br>This adds a digit to the end
 of the OTP generated to be used as a checksum to verify the OTP was generated correctly. This is in
 addition to the actual password length. You should only set this if your device supports it.",
      "propertyOrder" : 600,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "oathAlgorithm" : {
      "title" : "OATH Algorithm to Use",
      "description" : "Choose the algorithm your device uses to generate the OTP.<br><br>HOTP uses a
 counter value that is incremented every time a new OTP is generated. TOTP generates a new OTP every
 few seconds as specified by the time step interval.",
      "propertyOrder" : 400,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "oathIssuerName" : {
      "title" : "Name of the Issuer",
      "description" : "Name to identify the OTP issuer.",
      "propertyOrder" : 1100,
      "required" : true,
      "type" : "string",
      "exampleValue" : "ForgeRock"
    },
    "totpMaximumClockDrift" : {
      "title" : "Maximum Allowed Clock Drift",
      "description" : "Number of time steps a client is allowed to get out of sync with the server
 before manual resynchronisation is required. For example, with 3 allowed drifts and a time step
 interval of 30 seconds the server will allow codes from up to 90 seconds from the current time to be
 treated as the current time step. The drift for a user's device is calculated each time they enter a
 new code. If the drift exceeds this value, the user's authentication code will be rejected.",
```

```
     "propertyOrder" : 1000,
     "required" : true,
     "type" : "integer",
     "exampleValue" : ""
   },
   "hotpWindowSize" : {
     "title" : "HOTP Window Size",
     "description" : "The size of the window to resynchronize with the client.<br><br>This sets the
window that the OTP device and the server counter can be out of sync. For example, if the window size
is 100 and the servers last successful login was at counter value 2, then the server will accept a
OTP from the OTP device that is from device counter 3 to 102.",
     "propertyOrder" : 500,
     "required" : true,
     "type" : "integer",
     "exampleValue" : ""
   },
   "truncationOffset" : {
     "title" : "Truncation Offset",
     "description" : "This adds an offset to the generation of the OTP.<br><br>This is an option used
by the HOTP algorithm that not all devices support. This should be left default unless you know your
device uses a offset.",
     "propertyOrder" : 700,
     "required" : true,
     "type" : "integer",
     "exampleValue" : ""
   },
   "authenticationLevel" : {
     "title" : "Authentication Level",
     "description" : "The authentication level associated with this module.<br><br>Each
authentication module has an authentication level that can be used to indicate the level of security
associated with the module; 0 is the lowest (and the default).",
     "propertyOrder" : 100,
     "required" : true,
     "type" : "integer",
     "exampleValue" : ""
   },
   "totpTimeStepInterval" : {
     "title" : "TOTP Time Step Interval",
     "description" : "The TOTP time step in seconds that the OTP device uses to generate the
OTP.<br><br>This is the time interval that one OTP is valid for. For example, if the time step is 30
seconds, then a new OTP will be generated every 30 seconds. This makes a single OTP valid for only 30
seconds.",
     "propertyOrder" : 800,
     "required" : true,
     "type" : "integer",
     "exampleValue" : ""
   },
   "frOathOtpMaxRetry" : {
     "title" : "One Time Password Max Retry",
     "description" : "The number of times entry of the OTP may be attempted. Minimum is 1 maximum is
10 and default is 3.",
     "propertyOrder" : null,
     "required" : true,
     "type" : "integer",
     "exampleValue" : ""
   },
   "passwordLength" : {
     "title" : "One Time Password Length ",
```

```
      "description" : "The length of the generated OTP in digits, must be at least 6 and compatible
 with the hardware/software OTP generators you expect your end-users to use. For example, Google and
 ForgeRock authenticators support values of 6 and 8.",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "totpTimeStepsInWindow" : {
      "title" : "TOTP Time Steps",
      "description" : "The number of time steps to check before and after receiving a OTP.<br><br>This
 is the number of time step intervals to check the received OTP against both forward in time and back
 in time. For example, with 1 time steps and a time step interval of 30 seconds the server will allow
 a code between the previous code, the current code and the next code.",
      "propertyOrder" : 900,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    }
  }
}
```

Global Operations

Resource path: `/global-config/authentication/modules/authenticatoroath`

Resource version: `1.0`

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action AuthenticatorOathModule --global --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action AuthenticatorOathModule --global --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action AuthenticatorOathModule --global --actionName nextdescendents
```

read

Usage:

```
am> read AuthenticatorOathModule --global
```

update

Usage:

```
am> update AuthenticatorOathModule --global --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "defaults" : {
      "properties" : {
        "minimumSecretKeyLength" : {
          "title" : "Minimum Secret Key Length",
          "description" : "Number of hexadecimal characters allowed for the Secret Key.",
          "propertyOrder" : 300,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "passwordLength" : {
          "title" : "One Time Password Length ",
          "description" : "The length of the generated OTP in digits, must be at least 6 and
 compatible with the hardware/software OTP generators you expect your end-users to use. For example,
 Google and ForgeRock authenticators support values of 6 and 8.",
          "propertyOrder" : 200,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "totpTimeStepsInWindow" : {
          "title" : "TOTP Time Steps",
          "description" : "The number of time steps to check before and after receiving a
 OTP.<br><br>This is the number of time step intervals to check the received OTP against both forward
 in time and back in time. For example, with 1 time steps and a time step interval of 30 seconds the
 server will allow a code between the previous code, the current code and the next code.",
          "propertyOrder" : 900,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "addChecksumToOtpEnabled" : {
          "title" : "Add Checksum Digit",
```

```
          "description" : "This adds a checksum digit to the OTP.<br><br>This adds a digit to the end
of the OTP generated to be used as a checksum to verify the OTP was generated correctly. This is in
addition to the actual password length. You should only set this if your device supports it.",
          "propertyOrder" : 600,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "truncationOffset" : {
          "title" : "Truncation Offset",
          "description" : "This adds an offset to the generation of the OTP.<br><br>This is an option
used by the HOTP algorithm that not all devices support. This should be left default unless you know
your device uses a offset.",
          "propertyOrder" : 700,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "frOathOtpMaxRetry" : {
          "title" : "One Time Password Max Retry",
          "description" : "The number of times entry of the OTP may be attempted. Minimum is 1 maximum
is 10 and default is 3.",
          "propertyOrder" : null,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "authenticationLevel" : {
          "title" : "Authentication Level",
          "description" : "The authentication level associated with this module.<br><br>Each
authentication module has an authentication level that can be used to indicate the level of security
associated with the module; 0 is the lowest (and the default).",
          "propertyOrder" : 100,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "hotpWindowSize" : {
          "title" : "HOTP Window Size",
          "description" : "The size of the window to resynchronize with the client.<br><br>This sets
the window that the OTP device and the server counter can be out of sync. For example, if the window
size is 100 and the servers last successful login was at counter value 2, then the server will accept
a OTP from the OTP device that is from device counter 3 to 102.",
          "propertyOrder" : 500,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "totpTimeStepInterval" : {
          "title" : "TOTP Time Step Interval",
          "description" : "The TOTP time step in seconds that the OTP device uses to generate the
OTP.<br><br>This is the time interval that one OTP is valid for. For example, if the time step is 30
seconds, then a new OTP will be generated every 30 seconds. This makes a single OTP valid for only 30
seconds.",
          "propertyOrder" : 800,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
```

```
        "oathAlgorithm" : {
          "title" : "OATH Algorithm to Use",
          "description" : "Choose the algorithm your device uses to generate the OTP.<br><br>HOTP uses
 a counter value that is incremented every time a new OTP is generated. TOTP generates a new OTP every
 few seconds as specified by the time step interval.",
          "propertyOrder" : 400,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "totpMaximumClockDrift" : {
          "title" : "Maximum Allowed Clock Drift",
          "description" : "Number of time steps a client is allowed to get out of sync with the server
 before manual resynchronisation is required. For example, with 3 allowed drifts and a time step
 interval of 30 seconds the server will allow codes from up to 90 seconds from the current time to be
 treated as the current time step. The drift for a user's device is calculated each time they enter a
 new code. If the drift exceeds this value, the user's authentication code will be rejected.",
          "propertyOrder" : 1000,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "oathIssuerName" : {
          "title" : "Name of the Issuer",
          "description" : "Name to identify the OTP issuer.",
          "propertyOrder" : 1100,
          "required" : true,
          "type" : "string",
          "exampleValue" : "ForgeRock"
        }
      },
      "type" : "object",
      "title" : "Realm Defaults"
    }
  }
}
```


AuthenticatorPush

Realm Operations

Resource path: `/realm-config/services/authenticatorPushService`

Resource version: `1.0`

create

Usage:

```
am> create AuthenticatorPush --realm Realm --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "authenticatorPushDeviceSettingsEncryptionKeystorePassword" : {
      "title" : "Key Store Password",
      "description" : "Password to unlock the key store. This password is encrypted when it is saved
 in the OpenAM configuration. You should modify the default value.",
      "propertyOrder" : 500,
      "required" : true,
      "type" : "string",
      "format" : "password",
      "exampleValue" : ""
    },
    "authenticatorPushDeviceSettingsEncryptionKeystorePrivateKeyPassword" : {
      "title" : "Private Key Password",
      "description" : "Password to unlock the private key.",
      "propertyOrder" : 700,
      "required" : true,
      "type" : "string",
      "format" : "password",
      "exampleValue" : ""
    },
    "authenticatorPushDeviceSettingsEncryptionScheme" : {
      "title" : "Device Profile Encryption Scheme",
      "description" : "Encryption scheme to use to secure device profiles stored on the
 server.<br><br>If enabled, each device profile is encrypted using a unique random secret key
 using the given strength of AES encryption in CBC mode with PKCS#5 padding. An HMAC-SHA of the
 given strength (truncated to half-size) is used to ensure integrity protection and authenticated
 encryption. The unique random key is encrypted with the given RSA key pair and stored with the device
 profile.<p><p><i>Note:</i> AES-256 may require installation of the JCE Unlimited Strength policy
 files.",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "pushAttrName" : {
      "title" : "Profile Storage Attribute",
      "description" : "The user's attribute in which to store Push Notification profiles.<br><br>The
 default attribute is added to the schema when you prepare a user store for use with OpenAM. If you
 want to use a different attribute, you must make sure to add it to your user store schema prior to
 deploying push notifications with the ForgeRock Authenticator app in OpenAM. OpenAM must be able to
 write to the attribute.",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "authenticatorPushDeviceSettingsEncryptionKeystoreType" : {
      "title" : "Key Store Type",
      "description" : "Type of key store to load.<br><br><i>Note:</i> PKCS#11 key stores require
 hardware support such as a security device or smart card and is not available by default in most
```

```
 JVM installations.<p><p>See the <a href=\"https://docs.oracle.com/javase/8/docs/technotes/guides/
security/p11guide.html\" target=\"_blank\">JDK 8 PKCS#11 Reference Guide</a> for more details.",
      "propertyOrder" : 400,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "authenticatorPushDeviceSettingsEncryptionKeystoreKeyPairAlias" : {
      "title" : "Key-Pair Alias",
      "description" : "Alias of the certificate and private key in the key store. The private key is
 used to encrypt and decrypt device profiles.",
      "propertyOrder" : 600,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "authenticatorPushDeviceSettingsEncryptionKeystore" : {
      "title" : "Encryption Key Store",
      "description" : "Path to the key store from which to load encryption keys.",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "authenticatorPushSkippableName" : {
      "title" : "ForgeRock Authenticator (Push) Device Skippable Attribute Name",
      "description" : "Name of the attribute on a user's profile used to store their selection of
 whether to skip ForgeRock Authenticator (Push) 2FA modules.",
      "propertyOrder" : 800,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
```

delete

Usage:

```
am> delete AuthenticatorPush --realm Realm
```

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action AuthenticatorPush --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action AuthenticatorPush --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action AuthenticatorPush --realm Realm --actionName nextdescendents
```

read

Usage:

```
am> read AuthenticatorPush --realm Realm
```

update

Usage:

```
am> update AuthenticatorPush --realm Realm --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "authenticatorPushDeviceSettingsEncryptionKeystorePassword" : {
      "title" : "Key Store Password",
      "description" : "Password to unlock the key store. This password is encrypted when it is saved
 in the OpenAM configuration. You should modify the default value.",
      "propertyOrder" : 500,
      "required" : true,
      "type" : "string",
      "format" : "password",
      "exampleValue" : ""
    },
    "authenticatorPushDeviceSettingsEncryptionKeystorePrivateKeyPassword" : {
      "title" : "Private Key Password",
      "description" : "Password to unlock the private key.",
      "propertyOrder" : 700,
      "required" : true,
      "type" : "string",
      "format" : "password",
      "exampleValue" : ""
    },
    "authenticatorPushDeviceSettingsEncryptionScheme" : {
```

```
      "title" : "Device Profile Encryption Scheme",
      "description" : "Encryption scheme to use to secure device profiles stored on the
 server.<br><br>If enabled, each device profile is encrypted using a unique random secret key
 using the given strength of AES encryption in CBC mode with PKCS#5 padding. An HMAC-SHA of the
 given strength (truncated to half-size) is used to ensure integrity protection and authenticated
 encryption. The unique random key is encrypted with the given RSA key pair and stored with the device
 profile.<p><p><i>Note:</i> AES-256 may require installation of the JCE Unlimited Strength policy
 files.",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "pushAttrName" : {
      "title" : "Profile Storage Attribute",
      "description" : "The user's attribute in which to store Push Notification profiles.<br><br>The
 default attribute is added to the schema when you prepare a user store for use with OpenAM. If you
 want to use a different attribute, you must make sure to add it to your user store schema prior to
 deploying push notifications with the ForgeRock Authenticator app in OpenAM. OpenAM must be able to
 write to the attribute.",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "authenticatorPushDeviceSettingsEncryptionKeystoreType" : {
      "title" : "Key Store Type",
      "description" : "Type of key store to load.<br><br><i>Note:</i> PKCS#11 key stores require
 hardware support such as a security device or smart card and is not available by default in most
 JVM installations.<p><p>See the <a href=\"https://docs.oracle.com/javase/8/docs/technotes/guides/
security/p11guide.html\" target=\"_blank\">JDK 8 PKCS#11 Reference Guide</a> for more details.",
      "propertyOrder" : 400,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "authenticatorPushDeviceSettingsEncryptionKeystoreKeyPairAlias" : {
      "title" : "Key-Pair Alias",
      "description" : "Alias of the certificate and private key in the key store. The private key is
 used to encrypt and decrypt device profiles.",
      "propertyOrder" : 600,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "authenticatorPushDeviceSettingsEncryptionKeystore" : {
      "title" : "Encryption Key Store",
      "description" : "Path to the key store from which to load encryption keys.",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "authenticatorPushSkippableName" : {
      "title" : "ForgeRock Authenticator (Push) Device Skippable Attribute Name",
      "description" : "Name of the attribute on a user's profile used to store their selection of
 whether to skip ForgeRock Authenticator (Push) 2FA modules.",
      "propertyOrder" : 800,
      "required" : true,
```

```
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
```

Global Operations

Resource path: `/global-config/services/authenticatorPushService`

Resource version: `1.0`

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action AuthenticatorPush --global --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action AuthenticatorPush --global --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action AuthenticatorPush --global --actionName nextdescendents
```

read

Usage:

```
am> read AuthenticatorPush --global
```

update

Usage:

```
am> update AuthenticatorPush --global --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "defaults" : {
      "properties" : {
        "authenticatorPushDeviceSettingsEncryptionKeystorePassword" : {
          "title" : "Key Store Password",
          "description" : "Password to unlock the key store. This password is encrypted when it is
 saved in the OpenAM configuration. You should modify the default value.",
          "propertyOrder" : 500,
          "required" : true,
          "type" : "string",
          "format" : "password",
          "exampleValue" : ""
        },
        "authenticatorPushDeviceSettingsEncryptionScheme" : {
          "title" : "Device Profile Encryption Scheme",
          "description" : "Encryption scheme to use to secure device profiles stored on the
 server.<br><br>If enabled, each device profile is encrypted using a unique random secret key
 using the given strength of AES encryption in CBC mode with PKCS#5 padding. An HMAC-SHA of the
 given strength (truncated to half-size) is used to ensure integrity protection and authenticated
 encryption. The unique random key is encrypted with the given RSA key pair and stored with the device
 profile.<p><p><i>Note:</i> AES-256 may require installation of the JCE Unlimited Strength policy
 files.",
          "propertyOrder" : 200,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "authenticatorPushSkippableName" : {
          "title" : "ForgeRock Authenticator (Push) Device Skippable Attribute Name",
          "description" : "Name of the attribute on a user's profile used to store their selection of
 whether to skip ForgeRock Authenticator (Push) 2FA modules.",
          "propertyOrder" : 800,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "authenticatorPushDeviceSettingsEncryptionKeystoreType" : {
          "title" : "Key Store Type",
          "description" : "Type of key store to load.<br><br><i>Note:</i> PKCS#11 key stores require
 hardware support such as a security device or smart card and is not available by default in most
 JVM installations.<p><p>See the <a href=\"https://docs.oracle.com/javase/8/docs/technotes/guides/
security/p11guide.html\" target=\"_blank\">JDK 8 PKCS#11 Reference Guide</a> for more details.",
          "propertyOrder" : 400,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "authenticatorPushDeviceSettingsEncryptionKeystoreKeyPairAlias" : {
          "title" : "Key-Pair Alias",
          "description" : "Alias of the certificate and private key in the key store. The private key
 is used to encrypt and decrypt device profiles.",
```

```
          "propertyOrder" : 600,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "authenticatorPushDeviceSettingsEncryptionKeystorePrivateKeyPassword" : {
          "title" : "Private Key Password",
          "description" : "Password to unlock the private key.",
          "propertyOrder" : 700,
          "required" : true,
          "type" : "string",
          "format" : "password",
          "exampleValue" : ""
        },
        "authenticatorPushDeviceSettingsEncryptionKeystore" : {
          "title" : "Encryption Key Store",
          "description" : "Path to the key store from which to load encryption keys.",
          "propertyOrder" : 300,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "pushAttrName" : {
          "title" : "Profile Storage Attribute",
          "description" : "The user's attribute in which to store Push Notification
 profiles.<br><br>The default attribute is added to the schema when you prepare a user store for use
 with OpenAM. If you want to use a different attribute, you must make sure to add it to your user
 store schema prior to deploying push notifications with the ForgeRock Authenticator app in OpenAM.
 OpenAM must be able to write to the attribute.",
          "propertyOrder" : 100,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      },
      "type" : "object",
      "title" : "Realm Defaults"
    }
  }
}
```

AuthenticatorPushModule

Realm Operations

Resource path: `/realm-config/authentication/modules/authPush`

Resource version: `1.0`

create

Usage:

```
am> create AuthenticatorPushModule --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "timeoutInMilliSecconds" : {
      "title" : "Return Message Timeout (ms)",
      "description" : "The period of time (in milliseconds) within which a push notification should be
 replied to.",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "pushMessage" : {
      "title" : "Login Message",
      "description" : "Message transmitted over Push. Use the label {{user}} to replace with the
 registered login's username, and {{issuer}} to replace with the name of the issuer stored at
 registration.",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "authenticationLevel" : {
      "title" : "Authentication Level",
      "description" : "The authentication level associated with this module.<br><br>Each
 authentication module has an authentication level that can be used to indicate the level of security
 associated with the module; 0 is the lowest (and the default).",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    }
  }
}
```

delete

Usage:

```
am> delete AuthenticatorPushModule --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action AuthenticatorPushModule --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action AuthenticatorPushModule --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action AuthenticatorPushModule --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query AuthenticatorPushModule --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read AuthenticatorPushModule --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update AuthenticatorPushModule --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "timeoutInMilliSecconds" : {
      "title" : "Return Message Timeout (ms)",
      "description" : "The period of time (in milliseconds) within which a push notification should be
 replied to.",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "pushMessage" : {
      "title" : "Login Message",
      "description" : "Message transmitted over Push. Use the label {{user}} to replace with the
 registered login's username, and {{issuer}} to replace with the name of the issuer stored at
 registration.",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "authenticationLevel" : {
      "title" : "Authentication Level",
      "description" : "The authentication level associated with this module.<br><br>Each
 authentication module has an authentication level that can be used to indicate the level of security
 associated with the module; 0 is the lowest (and the default).",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    }
  }
}
```

Global Operations

Resource path: `/global-config/authentication/modules/authPush`

Resource version: `1.0`

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action AuthenticatorPushModule --global --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action AuthenticatorPushModule --global --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action AuthenticatorPushModule --global --actionName nextdescendents
```

read

Usage:

```
am> read AuthenticatorPushModule --global
```

update

Usage:

```
am> update AuthenticatorPushModule --global --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "defaults" : {
      "properties" : {
        "timeoutInMilliSecconds" : {
          "title" : "Return Message Timeout (ms)",
          "description" : "The period of time (in milliseconds) within which a push notification
 should be replied to.",
          "propertyOrder" : 200,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "authenticationLevel" : {
          "title" : "Authentication Level",
          "description" : "The authentication level associated with this module.<br><br>Each
 authentication module has an authentication level that can be used to indicate the level of security
 associated with the module; 0 is the lowest (and the default).",
          "propertyOrder" : 100,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "pushMessage" : {
          "title" : "Login Message",
          "description" : "Message transmitted over Push. Use the label {{user}} to replace with
 the registered login's username, and {{issuer}} to replace with the name of the issuer stored at
 registration.",
          "propertyOrder" : 300,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      },
      "type" : "object",
      "title" : "Realm Defaults"
    }
  }
}
```

AuthenticatorPushRegistrationModule

Realm Operations

Resource path: `/realm-config/authentication/modules/authPushReg`

Resource version: `1.0`

create

Usage:

```
am> create AuthenticatorPushRegistrationModule --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "appleLink" : {
      "title" : "App Store App URL",
      "description" : "URL of the app to download on the App Store.",
      "propertyOrder" : 600,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "googleLink" : {
      "title" : "Google Play URL",
      "description" : "URL of the app to download on Google Play.",
      "propertyOrder" : 700,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "timeoutInMilliSecconds" : {
      "title" : "Registration Response Timeout (ms)",
      "description" : "The period of time (in milliseconds) within which the registration QR code
 should be replied to.",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "issuer" : {
      "title" : "Issuer Name",
      "description" : "The Name of the service as it will appear on the registered device.",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "imgUrl" : {
      "title" : "Image URL",
      "description" : "The location of the image to download and display as your identity issuer's
 logo within the mobile app.",
```

```
      "propertyOrder" : 500,
      "required" : true,
      "type" : "string",
      "exampleValue" : "http://example.com/image.png"
    },
    "bgcolour" : {
      "title" : "Background Colour",
      "description" : "The background colour of the image to display behind your identity issuer's
 logo within the mobile app.",
      "propertyOrder" : 400,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "authenticationLevel" : {
      "title" : "Authentication Level",
      "description" : "The authentication level associated with this module.<br><br>Each
 authentication module has an authentication level that can be used to indicate the level of security
 associated with the module; 0 is the lowest (and the default).",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    }
  }
}
```

delete

Usage:

```
am> delete AuthenticatorPushRegistrationModule --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action AuthenticatorPushRegistrationModule --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action AuthenticatorPushRegistrationModule --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action AuthenticatorPushRegistrationModule --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query AuthenticatorPushRegistrationModule --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read AuthenticatorPushRegistrationModule --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update AuthenticatorPushRegistrationModule --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "appleLink" : {
      "title" : "App Store App URL",
      "description" : "URL of the app to download on the App Store.",
      "propertyOrder" : 600,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "googleLink" : {
      "title" : "Google Play URL",
      "description" : "URL of the app to download on Google Play.",
      "propertyOrder" : 700,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "timeoutInMilliSecconds" : {
      "title" : "Registration Response Timeout (ms)",
      "description" : "The period of time (in milliseconds) within which the registration QR code
 should be replied to.",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "issuer" : {
      "title" : "Issuer Name",
      "description" : "The Name of the service as it will appear on the registered device.",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "imgUrl" : {
      "title" : "Image URL",
      "description" : "The location of the image to download and display as your identity issuer's
 logo within the mobile app.",
      "propertyOrder" : 500,
      "required" : true,
      "type" : "string",
      "exampleValue" : "http://example.com/image.png"
    },
    "bgcolour" : {
      "title" : "Background Colour",
      "description" : "The background colour of the image to display behind your identity issuer's
 logo within the mobile app.",
      "propertyOrder" : 400,
```

```
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "authenticationLevel" : {
      "title" : "Authentication Level",
      "description" : "The authentication level associated with this module.<br><br>Each
 authentication module has an authentication level that can be used to indicate the level of security
 associated with the module; 0 is the lowest (and the default).",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    }
  }
}
```

Global Operations

Resource path: `/global-config/authentication/modules/authPushReg`

Resource version: `1.0`

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action AuthenticatorPushRegistrationModule --global --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action AuthenticatorPushRegistrationModule --global --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action AuthenticatorPushRegistrationModule --global --actionName nextdescendents
```

read

Usage:

```
am> read AuthenticatorPushRegistrationModule --global
```

update

Usage:

```
am> update AuthenticatorPushRegistrationModule --global --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "defaults" : {
      "properties" : {
        "issuer" : {
          "title" : "Issuer Name",
          "description" : "The Name of the service as it will appear on the registered device.",
          "propertyOrder" : 200,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "bgcolour" : {
          "title" : "Background Colour",
          "description" : "The background colour of the image to display behind your identity issuer's
 logo within the mobile app.",
          "propertyOrder" : 400,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "appleLink" : {
          "title" : "App Store App URL",
          "description" : "URL of the app to download on the App Store.",
          "propertyOrder" : 600,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "googleLink" : {
          "title" : "Google Play URL",
          "description" : "URL of the app to download on Google Play.",
          "propertyOrder" : 700,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "timeoutInMilliSecconds" : {
```

```
          "title" : "Registration Response Timeout (ms)",
          "description" : "The period of time (in milliseconds) within which the registration QR code
 should be replied to.",
          "propertyOrder" : 300,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "authenticationLevel" : {
          "title" : "Authentication Level",
          "description" : "The authentication level associated with this module.<br><br>Each
 authentication module has an authentication level that can be used to indicate the level of security
 associated with the module; 0 is the lowest (and the default).",
          "propertyOrder" : 100,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "imgUrl" : {
          "title" : "Image URL",
          "description" : "The location of the image to download and display as your identity issuer's
 logo within the mobile app.",
          "propertyOrder" : 500,
          "required" : true,
          "type" : "string",
          "exampleValue" : "http://example.com/image.png"
        }
      },
      "type" : "object",
      "title" : "Realm Defaults"
    }
  }
}
```


AuthenticatorWebAuthn

Realm Operations

Resource path: `/realm-config/services/authenticatorWebAuthnService`

Resource version: `1.0`

create

Usage:

```
am> create AuthenticatorWebAuthn --realm Realm --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "authenticatorWebAuthnDeviceSettingsEncryptionKeystorePrivateKeyPassword" : {
      "title" : "Private Key Password",
      "description" : "Password to unlock the private key.",
      "propertyOrder" : 700,
      "required" : true,
      "type" : "string",
      "format" : "password",
      "exampleValue" : ""
    },
    "authenticatorWebAuthnDeviceSettingsEncryptionKeystoreKeyPairAlias" : {
      "title" : "Key-Pair Alias",
      "description" : "Alias of the certificate and private key in the key store. The private key is
 used to encrypt and decrypt device profiles.",
      "propertyOrder" : 600,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "authenticatorWebAuthnDeviceSettingsEncryptionKeystore" : {
      "title" : "Encryption Key Store",
      "description" : "Path to the key store from which to load encryption keys.",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "authenticatorWebAuthnDeviceSettingsEncryptionScheme" : {
      "title" : "Device Profile Encryption Scheme",
      "description" : "Encryption scheme to use to secure device profiles stored on the
 server.<br><br>If enabled, each device profile is encrypted using a unique random secret key
 using the given strength of AES encryption in CBC mode with PKCS#5 padding. An HMAC-SHA of the
 given strength (truncated to half-size) is used to ensure integrity protection and authenticated
 encryption. The unique random key is encrypted with the given RSA key pair and stored with the device
 profile.<p><p><i>Note:</i> AES-256 may require installation of the JCE Unlimited Strength policy
 files.",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "authenticatorWebAuthnDeviceSettingsEncryptionKeystorePassword" : {
      "title" : "Key Store Password",
      "description" : "Password to unlock the key store. This password is encrypted when it is saved
 in the OpenAM configuration. You should modify the default value.",
      "propertyOrder" : 500,
      "required" : true,
      "type" : "string",
      "format" : "password",
      "exampleValue" : ""
    },
    "authenticatorWebAuthnDeviceSettingsEncryptionKeystoreType" : {
      "title" : "Key Store Type",
```

```
      "description" : "Type of key store to load.<br><br><i>Note:</i> PKCS#11 key stores require
 hardware support such as a security device or smart card and is not available by default in most
 JVM installations.<p><p>See the <a href=\"https://docs.oracle.com/javase/8/docs/technotes/guides/
security/p11guide.html\" target=\"_blank\">JDK 8 PKCS#11 Reference Guide</a> for more details.",
      "propertyOrder" : 400,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "webauthnAttrName" : {
      "title" : "Profile Storage Attribute",
      "description" : "The user's attribute in which to store WebAuthn profiles.<br><br>The default
 attribute is added to the schema when you prepare a user store for use with AM. If you want to use
 a different attribute, you must make sure to add it to your user store schema prior to deploying
 webauthn with AM. AM must be able to write to the attribute.",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
```

delete

Usage:

```
am> delete AuthenticatorWebAuthn --realm Realm
```

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action AuthenticatorWebAuthn --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action AuthenticatorWebAuthn --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action AuthenticatorWebAuthn --realm Realm --actionName nextdescendents
```

read

Usage:

```
am> read AuthenticatorWebAuthn --realm Realm
```

update

Usage:

```
am> update AuthenticatorWebAuthn --realm Realm --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "authenticatorWebAuthnDeviceSettingsEncryptionKeystorePrivateKeyPassword" : {
      "title" : "Private Key Password",
      "description" : "Password to unlock the private key.",
      "propertyOrder" : 700,
      "required" : true,
      "type" : "string",
      "format" : "password",
      "exampleValue" : ""
    },
    "authenticatorWebAuthnDeviceSettingsEncryptionKeystoreKeyPairAlias" : {
      "title" : "Key-Pair Alias",
      "description" : "Alias of the certificate and private key in the key store. The private key is
 used to encrypt and decrypt device profiles.",
      "propertyOrder" : 600,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "authenticatorWebAuthnDeviceSettingsEncryptionKeystore" : {
      "title" : "Encryption Key Store",
      "description" : "Path to the key store from which to load encryption keys.",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "authenticatorWebAuthnDeviceSettingsEncryptionScheme" : {
      "title" : "Device Profile Encryption Scheme",
      "description" : "Encryption scheme to use to secure device profiles stored on the
 server.<br><br>If enabled, each device profile is encrypted using a unique random secret key
 using the given strength of AES encryption in CBC mode with PKCS#5 padding. An HMAC-SHA of the
 given strength (truncated to half-size) is used to ensure integrity protection and authenticated
 encryption. The unique random key is encrypted with the given RSA key pair and stored with the device
 profile.<p><p><i>Note:</i> AES-256 may require installation of the JCE Unlimited Strength policy
 files.",
```

```
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "authenticatorWebAuthnDeviceSettingsEncryptionKeystorePassword" : {
      "title" : "Key Store Password",
      "description" : "Password to unlock the key store. This password is encrypted when it is saved
 in the OpenAM configuration. You should modify the default value.",
      "propertyOrder" : 500,
      "required" : true,
      "type" : "string",
      "format" : "password",
      "exampleValue" : ""
    },
    "authenticatorWebAuthnDeviceSettingsEncryptionKeystoreType" : {
      "title" : "Key Store Type",
      "description" : "Type of key store to load.<br><br><i>Note:</i> PKCS#11 key stores require
 hardware support such as a security device or smart card and is not available by default in most
 JVM installations.<p><p>See the <a href=\"https://docs.oracle.com/javase/8/docs/technotes/guides/
security/p11guide.html\" target=\"_blank\">JDK 8 PKCS#11 Reference Guide</a> for more details.",
      "propertyOrder" : 400,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "webauthnAttrName" : {
      "title" : "Profile Storage Attribute",
      "description" : "The user's attribute in which to store WebAuthn profiles.<br><br>The default
 attribute is added to the schema when you prepare a user store for use with AM. If you want to use
 a different attribute, you must make sure to add it to your user store schema prior to deploying
 webauthn with AM. AM must be able to write to the attribute.",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
```

Global Operations

Resource path: `/global-config/services/authenticatorWebAuthnService`

Resource version: `1.0`

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action AuthenticatorWebAuthn --global --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action AuthenticatorWebAuthn --global --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action AuthenticatorWebAuthn --global --actionName nextdescendents
```

read

Usage:

```
am> read AuthenticatorWebAuthn --global
```

update

Usage:

```
am> update AuthenticatorWebAuthn --global --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "defaults" : {
      "properties" : {
        "authenticatorWebAuthnDeviceSettingsEncryptionKeystorePassword" : {
          "title" : "Key Store Password",
          "description" : "Password to unlock the key store. This password is encrypted when it is
 saved in the OpenAM configuration. You should modify the default value.",
          "propertyOrder" : 500,
          "required" : true,
          "type" : "string",
          "format" : "password",
          "exampleValue" : ""
        },
        "authenticatorWebAuthnDeviceSettingsEncryptionKeystoreKeyPairAlias" : {
          "title" : "Key-Pair Alias",
          "description" : "Alias of the certificate and private key in the key store. The private key
 is used to encrypt and decrypt device profiles.",
```

```
          "propertyOrder" : 600,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "authenticatorWebAuthnDeviceSettingsEncryptionKeystoreType" : {
          "title" : "Key Store Type",
          "description" : "Type of key store to load.<br><br><i>Note:</i> PKCS#11 key stores require
 hardware support such as a security device or smart card and is not available by default in most
 JVM installations.<p><p>See the <a href=\"https://docs.oracle.com/javase/8/docs/technotes/guides/
security/p11guide.html\" target=\"_blank\">JDK 8 PKCS#11 Reference Guide</a> for more details.",
          "propertyOrder" : 400,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "authenticatorWebAuthnDeviceSettingsEncryptionKeystore" : {
          "title" : "Encryption Key Store",
          "description" : "Path to the key store from which to load encryption keys.",
          "propertyOrder" : 300,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "authenticatorWebAuthnDeviceSettingsEncryptionKeystorePrivateKeyPassword" : {
          "title" : "Private Key Password",
          "description" : "Password to unlock the private key.",
          "propertyOrder" : 700,
          "required" : true,
          "type" : "string",
          "format" : "password",
          "exampleValue" : ""
        },
        "authenticatorWebAuthnDeviceSettingsEncryptionScheme" : {
          "title" : "Device Profile Encryption Scheme",
          "description" : "Encryption scheme to use to secure device profiles stored on the
 server.<br><br>If enabled, each device profile is encrypted using a unique random secret key
 using the given strength of AES encryption in CBC mode with PKCS#5 padding. An HMAC-SHA of the
 given strength (truncated to half-size) is used to ensure integrity protection and authenticated
 encryption. The unique random key is encrypted with the given RSA key pair and stored with the device
 profile.<p><p><i>Note:</i> AES-256 may require installation of the JCE Unlimited Strength policy
 files.",
          "propertyOrder" : 200,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "webauthnAttrName" : {
          "title" : "Profile Storage Attribute",
          "description" : "The user's attribute in which to store WebAuthn profiles.<br><br>The
 default attribute is added to the schema when you prepare a user store for use with AM. If you
 want to use a different attribute, you must make sure to add it to your user store schema prior to
 deploying webauthn with AM. AM must be able to write to the attribute.",
          "propertyOrder" : 100,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      },
```

```
      "type" : "object",
      "title" : "Realm Defaults"
    }
  }
}
```

BaseUrlSource

Realm Operations

Resource path: `/realm-config/services/baseurl`

Resource version: `1.0`

create

Usage:

```
am> create BaseUrlSource --realm Realm --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "source" : {
      "title" : "Base URL Source",
      "description" : "Specifies the source of the base URL. Choose from the
following:<ul> <li>Extension class. Specifies that the extension class returns a
base URL from a provided HttpServletRequest. In the Extension class name field, enter
<code>org.forgerock.openam.services.baseurl.BaseURLProvider</code>.</li><li>Fixed value. Specifies
that the base URL is retrieved from a specific base URL value. In the Fixed value base URL field,
enter the base URL value.</li><li>Forwarded header. Specifies that the base URL is retrieved from
a forwarded header field in the HTTP request. The Forwarded HTTP header field is standardized and
specified in <a href=\"https://tools.ietf.org/html/rfc7239\">RFC7239</a>.</li><li>Host/protocol
from incoming request. Specifies that the hostname, server name, and port are retrieved from the
incoming HTTP request.</li><li>X-Forwarded-* headers. Specifies that the base URL is retrieved from
non-standard header fields, such as <code>X-Forwarded-For</code>, <code>X-Forwarded-By</code>, and
<code>X-Forwarded-Proto</code>.</li></ul>",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
```

```
    "contextPath" : {
      "title" : "Context path",
      "description" : "Specifies the context path for the base URL.<p><p>If provided, the base URL
 includes the deployment context path appended to the calculated URL.<p>For example, <code>/openam</
code>.",
      "propertyOrder" : 400,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "fixedValue" : {
      "title" : "Fixed value base URL",
      "description" : "If Fixed value is selected as the Base URL source, enter the base URL in the
 Fixed value base URL field.",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "extensionClassName" : {
      "title" : "Extension class name",
      "description" : "If Extension class is selected as the Base URL source, enter
 <code>org.forgerock.openam.services.baseurl.BaseURLProvider</code> in the Extension class name
 field.",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
```

delete

Usage:

```
am> delete BaseUrlSource --realm Realm
```

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action BaseUrlSource --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action BaseUrlSource --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action BaseUrlSource --realm Realm --actionName nextdescendents
```

read

Usage:

```
am> read BaseUrlSource --realm Realm
```

update

Usage:

```
am> update BaseUrlSource --realm Realm --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "source" : {
      "title" : "Base URL Source",
      "description" : "Specifies the source of the base URL. Choose from the
 following:<ul> <li>Extension class. Specifies that the extension class returns a
 base URL from a provided HttpServletRequest. In the Extension class name field, enter
 <code>org.forgerock.openam.services.baseurl.BaseURLProvider</code>.</li><li>Fixed value. Specifies
 that the base URL is retrieved from a specific base URL value. In the Fixed value base URL field,
 enter the base URL value.</li><li>Forwarded header. Specifies that the base URL is retrieved from
 a forwarded header field in the HTTP request. The Forwarded HTTP header field is standardized and
 specified in <a href=\"https://tools.ietf.org/html/rfc7239\">RFC7239</a>.</li><li>Host/protocol
 from incoming request. Specifies that the hostname, server name, and port are retrieved from the
 incoming HTTP request.</li><li>X-Forwarded-* headers. Specifies that the base URL is retrieved from
 non-standard header fields, such as <code>X-Forwarded-For</code>, <code>X-Forwarded-By</code>, and
 <code>X-Forwarded-Proto</code>.</li></ul>",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
```

```
    "contextPath" : {
      "title" : "Context path",
      "description" : "Specifies the context path for the base URL.<p><p>If provided, the base URL
 includes the deployment context path appended to the calculated URL.<p>For example, <code>/openam</
code>.",
      "propertyOrder" : 400,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "fixedValue" : {
      "title" : "Fixed value base URL",
      "description" : "If Fixed value is selected as the Base URL source, enter the base URL in the
 Fixed value base URL field.",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "extensionClassName" : {
      "title" : "Extension class name",
      "description" : "If Extension class is selected as the Base URL source, enter
 <code>org.forgerock.openam.services.baseurl.BaseURLProvider</code> in the Extension class name
 field.",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
```

Global Operations

Resource path: `/global-config/services/baseurl`

Resource version: `1.0`

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action BaseUrlSource --global --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action BaseUrlSource --global --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action BaseUrlSource --global --actionName nextdescendents
```

read

Usage:

```
am> read BaseUrlSource --global
```

update

Usage:

```
am> update BaseUrlSource --global --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "defaults" : {
      "properties" : {
        "contextPath" : {
          "title" : "Context path",
          "description" : "Specifies the context path for the base URL.<p><p>If provided, the base URL
 includes the deployment context path appended to the calculated URL.<p>For example, <code>/openam</
code>.",
          "propertyOrder" : 400,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "source" : {
          "title" : "Base URL Source",
          "description" : "Specifies the source of the base URL. Choose from the
 following:<ul> <li>Extension class. Specifies that the extension class returns a
 base URL from a provided HttpServletRequest. In the Extension class name field, enter
 <code>org.forgerock.openam.services.baseurl.BaseURLProvider</code>.</li><li>Fixed value. Specifies
 that the base URL is retrieved from a specific base URL value. In the Fixed value base URL field,
```

```
 enter the base URL value.</li><li>Forwarded header. Specifies that the base URL is retrieved from
 a forwarded header field in the HTTP request. The Forwarded HTTP header field is standardized and
 specified in <a href=\"https://tools.ietf.org/html/rfc7239\">RFC7239</a>.</li><li>Host/protocol
 from incoming request. Specifies that the hostname, server name, and port are retrieved from the
 incoming HTTP request.</li><li>X-Forwarded-* headers. Specifies that the base URL is retrieved from
 non-standard header fields, such as <code>X-Forwarded-For</code>, <code>X-Forwarded-By</code>, and
 <code>X-Forwarded-Proto</code>.</li></ul>",
          "propertyOrder" : 100,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "extensionClassName" : {
          "title" : "Extension class name",
          "description" : "If Extension class is selected as the Base URL source, enter
 <code>org.forgerock.openam.services.baseurl.BaseURLProvider</code> in the Extension class name
 field.",
          "propertyOrder" : 300,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "fixedValue" : {
          "title" : "Fixed value base URL",
          "description" : "If Fixed value is selected as the Base URL source, enter the base URL in
 the Fixed value base URL field.",
          "propertyOrder" : 200,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      },
      "type" : "object",
      "title" : "Realm Defaults"
    }
  }
}
```

CORSService

Global Operations

Resource path: `/global-config/services/CorsService`

Resource version: `1.0`

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action CORSService --global --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action CORSService --global --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action CORSService --global --actionName nextdescendents
```

read

Usage:

```
am> read CORSService --global
```

update

Usage:

```
am> update CORSService --global --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "enabled" : {
      "title" : "Enable the CORS filter",
      "description" : "If disable, no CORS headers will be added to responses.",
      "propertyOrder" : 1,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    }
  }
}
```

CRESTReporter

Global Operations

Resource path: `/global-config/services/monitoring/crest`

Resource version: `1.0`

create

Usage:

```
am> create CRESTReporter --global --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "enabled" : {
      "title" : "Enabled",
      "description" : "",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    }
  }
}
```

delete

Usage:

```
am> delete CRESTReporter --global --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action CRESTReporter --global --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action CRESTReporter --global --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action CRESTReporter --global --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query CRESTReporter --global --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read CRESTReporter --global --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update CRESTReporter --global --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "enabled" : {
      "title" : "Enabled",
      "description" : "",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    }
  }
}
```

Captcha

Realm Operations

Resource path: `/realm-config/authentication/authenticationtrees/nodes/product-ReCaptchaNode`

Resource version: `1.0`

create

Usage:

```
am> create Captcha --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "reCaptchaUri" : {
      "title" : "CAPTCHA Verification URL",
      "description" : "URL to Verify CAPTCHA, defaults to the Google ReCAPTCHA verification URI.",
      "propertyOrder" : 300,
      "type" : "string",
      "exampleValue" : ""
    },
    "divClass" : {
      "title" : "Class of CAPTCHA HTML <div>",
      "description" : "The class of the HTML <div> element required by the captcha API, defaults to
 Google the ReCAPTCHA <div>.",
      "propertyOrder" : 500,
      "type" : "string",
      "exampleValue" : ""
    },
    "secretKey" : {
      "title" : "CAPTCHA Secret Key",
      "description" : "CAPTCHA Secret Key",
      "propertyOrder" : 200,
      "type" : "string",
      "exampleValue" : ""
    },
    "siteKey" : {
      "title" : "CAPTCHA Site Key",
      "description" : "CAPTCHA Site Key",
      "propertyOrder" : 100,
      "type" : "string",
      "exampleValue" : ""
    },
    "apiUri" : {
      "title" : "CAPTCHA API URL",
      "description" : "The URL of the JavaScript to load the CAPTCHA verification, defaults to the
 Google ReCAPTCHA API.",
      "propertyOrder" : 400,
      "type" : "string",
      "exampleValue" : ""
    }
  },
  "required" : [ "apiUri", "reCaptchaUri", "siteKey", "divClass", "secretKey" ]
}
```

delete

Usage:

```
am> delete Captcha --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action Captcha --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action Captcha --realm Realm --actionName getCreatableTypes
```

listOutcomes

List the available outcomes for the node type.

Usage:

```
am> action Captcha --realm Realm --body body --actionName listOutcomes
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "title" : "Some configuration of the node. This does not need to be complete against the
 configuration schema."
}
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action Captcha --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query Captcha --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read Captcha --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update Captcha --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "reCaptchaUri" : {
      "title" : "CAPTCHA Verification URL",
```

```
      "description" : "URL to Verify CAPTCHA, defaults to the Google ReCAPTCHA verification URI.",
      "propertyOrder" : 300,
      "type" : "string",
      "exampleValue" : ""
    },
    "divClass" : {
      "title" : "Class of CAPTCHA HTML <div>",
      "description" : "The class of the HTML <div> element required by the captcha API, defaults to
 Google the ReCAPTCHA <div>.",
      "propertyOrder" : 500,
      "type" : "string",
      "exampleValue" : ""
    },
    "secretKey" : {
      "title" : "CAPTCHA Secret Key",
      "description" : "CAPTCHA Secret Key",
      "propertyOrder" : 200,
      "type" : "string",
      "exampleValue" : ""
    },
    "siteKey" : {
      "title" : "CAPTCHA Site Key",
      "description" : "CAPTCHA Site Key",
      "propertyOrder" : 100,
      "type" : "string",
      "exampleValue" : ""
    },
    "apiUri" : {
      "title" : "CAPTCHA API URL",
      "description" : "The URL of the JavaScript to load the CAPTCHA verification, defaults to the
 Google ReCAPTCHA API.",
      "propertyOrder" : 400,
      "type" : "string",
      "exampleValue" : ""
    }
  },
  "required" : [ "apiUri", "reCaptchaUri", "siteKey", "divClass", "secretKey" ]
}
```

CertificateCollectorNode

Realm Operations

Resource path: `/realm-config/authentication/authenticationtrees/nodes/product-CertificateCollectorNode`

Resource version: `1.0`

create

Usage:

```
am> create CertificateCollectorNode --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "clientCertificateHttpHeaderName" : {
      "title" : "HTTP Header Name for Client Certificate",
      "description" : "The name of the HTTP request header containing the certificate, only used when
 header based collection is enabled.",
      "propertyOrder" : 200,
      "type" : "string",
      "exampleValue" : ""
    },
    "trustedRemoteHosts" : {
      "title" : "Trusted Remote Hosts",
      "description" : "A list of IP addresses trusted to supply client certificates.<br><br>If SSL/
TLS is being terminated at a load balancer or at the Distributed Authentication server then this
 option can be used to ensure that only specified trusted hosts (identified by IP address) are allowed
 to supply client certificates to the certificate node.<br><br>Empty list means do not trust remote
 headers and a single value of \"any\" means all are trusted <code>any</code>.",
      "propertyOrder" : 300,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "certificateCollectionMethod" : {
      "title" : "Certificate Collection Method",
      "description" : "This field defines how the certificate should be client certificate should
 be collected from the request. If TLS termination happens at the web container that is running
 Access Management, choose <code>Request</code>. If you have Access Management behind a proxy or load
 balancer and terminate TLS there, select <code>Header</code>. If <code>Either</code> is selected,
 the collector node will first look at the request, then look at the <code>HTTP Header Name for Client
 Certificate</code> specified in that order.",
      "propertyOrder" : 100,
      "type" : "string",
      "exampleValue" : ""
    }
  },
  "required" : [ "certificateCollectionMethod", "trustedRemoteHosts" ]
}
```

delete

Usage:

```
am> delete CertificateCollectorNode --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action CertificateCollectorNode --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action CertificateCollectorNode --realm Realm --actionName getCreatableTypes
```

listOutcomes

List the available outcomes for the node type.

Usage:

```
am> action CertificateCollectorNode --realm Realm --body body --actionName listOutcomes
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "title" : "Some configuration of the node. This does not need to be complete against the
 configuration schema."
}
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action CertificateCollectorNode --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query CertificateCollectorNode --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read CertificateCollectorNode --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update CertificateCollectorNode --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "clientCertificateHttpHeaderName" : {
      "title" : "HTTP Header Name for Client Certificate",
      "description" : "The name of the HTTP request header containing the certificate, only used when
 header based collection is enabled.",
      "propertyOrder" : 200,
      "type" : "string",
      "exampleValue" : ""
    },
    "trustedRemoteHosts" : {
      "title" : "Trusted Remote Hosts",
      "description" : "A list of IP addresses trusted to supply client certificates.<br><br>If SSL/
TLS is being terminated at a load balancer or at the Distributed Authentication server then this
 option can be used to ensure that only specified trusted hosts (identified by IP address) are allowed
 to supply client certificates to the certificate node.<br><br>Empty list means do not trust remote
 headers and a single value of \"any\" means all are trusted <code>any</code>.",
      "propertyOrder" : 300,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "certificateCollectionMethod" : {
      "title" : "Certificate Collection Method",
      "description" : "This field defines how the certificate should be client certificate should
 be collected from the request. If TLS termination happens at the web container that is running
 Access Management, choose <code>Request</code>. If you have Access Management behind a proxy or load
 balancer and terminate TLS there, select <code>Header</code>. If <code>Either</code> is selected,
 the collector node will first look at the request, then look at the <code>HTTP Header Name for Client
 Certificate</code> specified in that order.",
      "propertyOrder" : 100,
      "type" : "string",
      "exampleValue" : ""
    }
  },
  "required" : [ "certificateCollectionMethod", "trustedRemoteHosts" ]
}
```


CertificateModule

Realm Operations

Resource path: `/realm-config/authentication/modules/certificate`

Resource version: `1.0`

create

Usage:

```
am> create CertificateModule --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "matchCertificateInLdap" : {
      "title" : "Match Certificate in LDAP",
      "description" : "The client certificate must exist in the directory for the authentication to be
 successful.",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "certificateAttributeProfileMappingExtension" : {
      "title" : "SubjectAltNameExt Value Type to Access User Profile",
      "description" : "Use the Subject Alternative Name Field in preference to one of the standard
 certificate fields.<br><br>Selecting RFC822Name or UPN will cause this field to have have precedence
 over the <i>Certificate Field Used to Access User Profile</i> or <i>Other Certificate Field Used
 to Access User Profile</i> attribute.<br/><br/><i>NB </i>The client certificate must contain the
 <i>Subject Alternate Name Extension</i> for this function to operate.",
      "propertyOrder" : 1700,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "updateCRLsFromDistributionPoint" : {
      "title" : "Update CA CRLs from CRLDistributionPoint",
      "description" : "Fetch new CA CRLs from CRLDistributionPoint and update it in
 Directory Server<br><br>If the CA certificate includes an IssuingDistributionPoint or has an
 CRLDistributionPoint extension set OpenAM tries to update the CRLs if neeed (i.e. CRL is out-of-
date). <br/>This property controls if the update should be performed.<br/>This property is only used
 if CA CRL checking is enabled.",
      "propertyOrder" : 800,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "iplanet-am-auth-cert-gw-cert-preferred" : {
      "title" : "Use only Certificate from HTTP request header",
      "description" : "Strictly use client cert from HTTP header over cert from HTTPS connection/
servlet attribute",
      "propertyOrder" : 2000,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
```

```
    "certificateLdapServers" : {
      "title" : "LDAP Server Where Certificates are Stored",
      "description" : "Use this list to set the LDAP server used to search for certificates.
 <br><br>The Certificate authentication module will use this list for the LDAP server used to search
 for certificates. A single entry must be in the format:<br/><br/><code>ldap_server:port</code><br/
><br/>Multiple entries allow associations between OpenAM servers and a LDAP server. The format is:<br/
><br/><code>local server name | server:port</code><br/><br/>The local server name is the full name of
 the server from the list of servers and sites.",
      "propertyOrder" : 1000,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "otherCertificateAttributeToProfileMapping" : {
      "title" : "Other Certificate Field Used to Access User Profile",
      "description" : "This field is only used if the <i>Certificate Field Used to Access User
 Profile</i> attribute is set to <i>other</i>. This field allows a custom certificate field to be used
 as the basis of the user search.",
      "propertyOrder" : 1600,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "crlHttpParameters" : {
      "title" : "HTTP Parameters for CRL Update",
      "description" : "These parameters will be included in any HTTP CRL call to the Certificate
 Authority<br><br>If the Client or CA certificate contains the Issuing Distribution Point Extension
 then OpenAM will use this information to retrieve the CRL from the distribution point. This property
 allow custom HTTP parameters to be included in the CRL request.<br/><br/>The format of the parameter
 is as follows:<br/><br/><code>param1=value1,param2=value</code>",
      "propertyOrder" : 500,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "sslEnabled" : {
      "title" : "Use SSL/TLS for LDAP Access",
      "description" : "The certificate module will use SSL/TLS to access the LDAP server",
      "propertyOrder" : 1400,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "matchCertificateToCRL" : {
      "title" : "Match Certificate to CRL",
      "description" : "The Client Certificate will be checked against the Certificate Revocation list
 held in the directory<br><br>A Certificate Revocation List can be provisioned into the directory.
 Having this option enabled will cause all client certificates to be checked against this list.",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "authenticationLevel" : {
      "title" : "Authentication Level",
```

```
      "description" : "The authentication level associated with this module.<br><br>Each
 authentication module has an authentication level that can be used to indicate the level of security
 associated with the module; 0 is the lowest (and the default).",
      "propertyOrder" : 2100,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "matchCACertificateToCRL" : {
      "title" : "Match CA Certificate to CRL",
      "description" : "The CA certificate that issued the client certificate will also be checked
 against the CRL.",
      "propertyOrder" : 600,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "ldapSearchStartDN" : {
      "title" : "LDAP Search Start or Base DN",
      "description" : "The start point in the LDAP server for the certificate search<br><br>When
 entering multiple entries, each entry must be prefixed with a local server name. Multiple entries
 allow different search Base DNs depending on the OpenAM server in use. The format is:<br/><br/
><code>local server name | base dn</code><br/><br/>The local server name is the full name of the
 server from the list of servers and sites.",
      "propertyOrder" : 1100,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "trustedRemoteHosts" : {
      "title" : "Trusted Remote Hosts",
      "description" : "A list of IP addresses trusted to supply client certificates.<br><br>If SSL/TLS
 is being terminated at a load balancer or at the Distributed Authentication server then this option
 can be used to ensure that only specified <i>trusted</i> hosts (identified by IP address) are allowed
 to supply client certificates to the certificate module,<br/><br/>Valid values for this list are as
 follows:<ul><li>none</li><li>any</li><li>multiple IP addresses</li></ul><br/><br/>The default value
 of <i>none</i> disables this functionality",
      "propertyOrder" : 1800,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "ocspValidationEnabled" : {
      "title" : "OCSP Validation",
      "description" : "Enable Online Certificate Status Protocol validation for OCSP aware
 certificates<br><br>If the certificate contains OCSP validation information then OpenAM will use this
 information to check the validity of the certificate as part of the authentication process.<br/><br/
><i>NB </i>The OpenAM server must have Internet connectivity for OCSP to work",
      "propertyOrder" : 900,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
```

```
   "userBindPassword" : {
     "title" : "LDAP Server Authentication Password",
     "description" : "The password for the authentication user",
     "propertyOrder" : 1300,
     "required" : true,
     "type" : "string",
     "format" : "password",
     "exampleValue" : ""
   },
   "certificateAttributeToProfileMapping" : {
     "title" : "Certificate Field Used to Access User Profile",
     "description" : "The certificate module needs to read a value from the client certificate that
can be used to search the LDAP server for a matching certificate.  ",
     "propertyOrder" : 1500,
     "required" : true,
     "type" : "string",
     "exampleValue" : ""
   },
   "cacheCRLsInMemory" : {
     "title" : "Cache CRLs in memory",
     "description" : "The CRLs will be cached in memory",
     "propertyOrder" : 700,
     "required" : true,
     "type" : "boolean",
     "exampleValue" : ""
   },
   "clientCertificateHttpHeaderName" : {
     "title" : "HTTP Header Name for Client Certificate",
     "description" : "The name of the HTTP request header containing the certificate, only used when
<i>Trusted Remote Hosts</i> mode is enabled.",
     "propertyOrder" : 1900,
     "required" : true,
     "type" : "string",
     "exampleValue" : ""
   },
   "crlMatchingCertificateAttribute" : {
     "title" : "Issuer DN Attribute(s) Used to Search LDAP for CRLs",
     "description" : "This is the name of the attribute taken from the CA certificate that will
be used to search the CRL.<br><br>If only one attribute name is specified, the ldap searchfilter
will be (attrName=Value_of_the_corresponding_Attribute_from_SubjectDN)<br/>e.g. SubjectDN of issuer
cert 'C=US, CN=Some CA, serialNumber=123456',attribute name specified is 'CN', searchfilter used
will be <code>(CN=Some CA)</code><br/><br/>If serveral attribute names are specified, they have
to separated by <code>,</code>. The resulting ldap searchfilter value will be a comma separated
list of name attribute values, the search attribute will be <code>cn</code><br/>e.g. SubjectDN of
issuer cert 'C=US, CN=Some CA, serialNumber=123456',attribute names specified are 'CN,serialNumber',
searchfilter used will be <code>cn=CN=Some CA,serialNumber=123456</code><br/>The order of the values
of the attribute names matter as they must match the value of the <code>cn</code> attribute of a
crlDistributionPoint entry in the directory server.",
     "propertyOrder" : 400,
     "required" : true,
     "type" : "string",
     "exampleValue" : ""
   },
   "ldapCertificateAttribute" : {
     "title" : "Subject DN Attribute Used to Search LDAP for Certificates",
     "description" : "This is the attribute used to search the directory for the
certificate<br><br>The Certificate module will search the directory for the certificate using the
search filter based on this attribute and the value of the Subject DN taken from the certificate.",
     "propertyOrder" : 200,
```

```
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "userBindDN" : {
      "title" : "LDAP Server Authentication User",
      "description" : "DN of the user used by the module to authenticate to the LDAP server<br><br>The
 Certificate module authenticates to the LDAP server in order to search for a matching certificate.
 The DN entered here represents the account used for said authentication and must have read/search
 access to the LDAP server.",
      "propertyOrder" : 1200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
```

delete

Usage:

```
am> delete CertificateModule --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action CertificateModule --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action CertificateModule --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action CertificateModule --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query CertificateModule --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read CertificateModule --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update CertificateModule --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "matchCertificateInLdap" : {
      "title" : "Match Certificate in LDAP",
      "description" : "The client certificate must exist in the directory for the authentication to be
 successful.",
      "propertyOrder" : 100,
```

```
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "certificateAttributeProfileMappingExtension" : {
      "title" : "SubjectAltNameExt Value Type to Access User Profile",
      "description" : "Use the Subject Alternative Name Field in preference to one of the standard
 certificate fields.<br><br>Selecting RFC822Name or UPN will cause this field to have have precedence
 over the <i>Certificate Field Used to Access User Profile</i> or <i>Other Certificate Field Used
 to Access User Profile</i> attribute.<br/><br/><i>NB </i>The client certificate must contain the
 <i>Subject Alternate Name Extension</i> for this function to operate.",
      "propertyOrder" : 1700,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "updateCRLsFromDistributionPoint" : {
      "title" : "Update CA CRLs from CRLDistributionPoint",
      "description" : "Fetch new CA CRLs from CRLDistributionPoint and update it in
 Directory Server<br><br>If the CA certificate includes an IssuingDistributionPoint or has an
 CRLDistributionPoint extension set OpenAM tries to update the CRLs if neeed (i.e. CRL is out-of-
date). <br/>This property controls if the update should be performed.<br/>This property is only used
 if CA CRL checking is enabled.",
      "propertyOrder" : 800,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "iplanet-am-auth-cert-gw-cert-preferred" : {
      "title" : "Use only Certificate from HTTP request header",
      "description" : "Strictly use client cert from HTTP header over cert from HTTPS connection/
servlet attribute",
      "propertyOrder" : 2000,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "certificateLdapServers" : {
      "title" : "LDAP Server Where Certificates are Stored",
      "description" : "Use this list to set the LDAP server used to search for certificates.
 <br><br>The Certificate authentication module will use this list for the LDAP server used to search
 for certificates. A single entry must be in the format:<br/><br/><code>ldap_server:port</code><br/
><br/>Multiple entries allow associations between OpenAM servers and a LDAP server. The format is:<br/
><br/><code>local server name | server:port</code><br/><br/>The local server name is the full name of
 the server from the list of servers and sites.",
      "propertyOrder" : 1000,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "otherCertificateAttributeToProfileMapping" : {
      "title" : "Other Certificate Field Used to Access User Profile",
      "description" : "This field is only used if the <i>Certificate Field Used to Access User
 Profile</i> attribute is set to <i>other</i>. This field allows a custom certificate field to be used
 as the basis of the user search.",
      "propertyOrder" : 1600,
```

```
     "required" : true,
     "type" : "string",
     "exampleValue" : ""
   },
   "crlHttpParameters" : {
     "title" : "HTTP Parameters for CRL Update",
     "description" : "These parameters will be included in any HTTP CRL call to the Certificate
Authority<br><br>If the Client or CA certificate contains the Issuing Distribution Point Extension
then OpenAM will use this information to retrieve the CRL from the distribution point. This property
allow custom HTTP parameters to be included in the CRL request.<br/><br/>The format of the parameter
is as follows:<br/><br/><code>param1=value1,param2=value</code>",
     "propertyOrder" : 500,
     "required" : true,
     "type" : "string",
     "exampleValue" : ""
   },
   "sslEnabled" : {
     "title" : "Use SSL/TLS for LDAP Access",
     "description" : "The certificate module will use SSL/TLS to access the LDAP server",
     "propertyOrder" : 1400,
     "required" : true,
     "type" : "boolean",
     "exampleValue" : ""
   },
   "matchCertificateToCRL" : {
     "title" : "Match Certificate to CRL",
     "description" : "The Client Certificate will be checked against the Certificate Revocation list
held in the directory<br><br>A Certificate Revocation List can be provisioned into the directory.
Having this option enabled will cause all client certificates to be checked against this list.",
     "propertyOrder" : 300,
     "required" : true,
     "type" : "boolean",
     "exampleValue" : ""
   },
   "authenticationLevel" : {
     "title" : "Authentication Level",
     "description" : "The authentication level associated with this module.<br><br>Each
authentication module has an authentication level that can be used to indicate the level of security
associated with the module; 0 is the lowest (and the default).",
     "propertyOrder" : 2100,
     "required" : true,
     "type" : "integer",
     "exampleValue" : ""
   },
   "matchCACertificateToCRL" : {
     "title" : "Match CA Certificate to CRL",
     "description" : "The CA certificate that issued the client certificate will also be checked
against the CRL.",
     "propertyOrder" : 600,
     "required" : true,
     "type" : "boolean",
     "exampleValue" : ""
   },
   "ldapSearchStartDN" : {
     "title" : "LDAP Search Start or Base DN",
     "description" : "The start point in the LDAP server for the certificate search<br><br>When
entering multiple entries, each entry must be prefixed with a local server name. Multiple entries
allow different search Base DNs depending on the OpenAM server in use. The format is:<br/><br/>
```

```
><code>local server name | base dn</code><br/><br/>The local server name is the full name of the
 server from the list of servers and sites.",
      "propertyOrder" : 1100,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "trustedRemoteHosts" : {
      "title" : "Trusted Remote Hosts",
      "description" : "A list of IP addresses trusted to supply client certificates.<br><br>If SSL/TLS
 is being terminated at a load balancer or at the Distributed Authentication server then this option
 can be used to ensure that only specified <i>trusted</i> hosts (identified by IP address) are allowed
 to supply client certificates to the certificate module,<br/><br/>Valid values for this list are as
 follows:<ul><li>none</li><li>any</li><li>multiple IP addresses</li></ul><br/><br/>The default value
 of <i>none</i> disables this functionality",
      "propertyOrder" : 1800,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "ocspValidationEnabled" : {
      "title" : "OCSP Validation",
      "description" : "Enable Online Certificate Status Protocol validation for OCSP aware
 certificates<br><br>If the certificate contains OCSP validation information then OpenAM will use this
 information to check the validity of the certificate as part of the authentication process.<br/><br/
><i>NB </i>The OpenAM server must have Internet connectivity for OCSP to work",
      "propertyOrder" : 900,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "userBindPassword" : {
      "title" : "LDAP Server Authentication Password",
      "description" : "The password for the authentication user",
      "propertyOrder" : 1300,
      "required" : true,
      "type" : "string",
      "format" : "password",
      "exampleValue" : ""
    },
    "certificateAttributeToProfileMapping" : {
      "title" : "Certificate Field Used to Access User Profile",
      "description" : "The certificate module needs to read a value from the client certificate that
 can be used to search the LDAP server for a matching certificate.  ",
      "propertyOrder" : 1500,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "cacheCRLsInMemory" : {
      "title" : "Cache CRLs in memory",
      "description" : "The CRLs will be cached in memory",
      "propertyOrder" : 700,
```

```
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "clientCertificateHttpHeaderName" : {
      "title" : "HTTP Header Name for Client Certificate",
      "description" : "The name of the HTTP request header containing the certificate, only used when
 <i>Trusted Remote Hosts</i> mode is enabled.",
      "propertyOrder" : 1900,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "crlMatchingCertificateAttribute" : {
      "title" : "Issuer DN Attribute(s) Used to Search LDAP for CRLs",
      "description" : "This is the name of the attribute taken from the CA certificate that will
 be used to search the CRL.<br><br>If only one attribute name is specified, the ldap searchfilter
 will be (attrName=Value_of_the_corresponding_Attribute_from_SubjectDN)<br/>e.g. SubjectDN of issuer
 cert 'C=US, CN=Some CA, serialNumber=123456',attribute name specified is 'CN', searchfilter used
 will be <code>(CN=Some CA)</code><br/><br/>If serveral attribute names are specified, they have
 to separated by <code>,</code>. The resulting ldap searchfilter value will be a comma separated
 list of name attribute values, the search attribute will be <code>cn</code><br/>e.g. SubjectDN of
 issuer cert 'C=US, CN=Some CA, serialNumber=123456',attribute names specified are 'CN,serialNumber',
 searchfilter used will be <code>cn=CN=Some CA,serialNumber=123456</code><br/>The order of the values
 of the attribute names matter as they must match the value of the <code>cn</code> attribute of a
 crlDistributionPoint entry in the directory server.",
      "propertyOrder" : 400,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "ldapCertificateAttribute" : {
      "title" : "Subject DN Attribute Used to Search LDAP for Certificates",
      "description" : "This is the attribute used to search the directory for the
 certificate<br><br>The Certificate module will search the directory for the certificate using the
 search filter based on this attribute and the value of the Subject DN taken from the certificate.",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "userBindDN" : {
      "title" : "LDAP Server Authentication User",
      "description" : "DN of the user used by the module to authenticate to the LDAP server<br><br>The
 Certificate module authenticates to the LDAP server in order to search for a matching certificate.
 The DN entered here represents the account used for said authentication and must have read/search
 access to the LDAP server.",
      "propertyOrder" : 1200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
```

Global Operations

Resource path: `/global-config/authentication/modules/certificate`

Resource version: `1.0`

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action CertificateModule --global --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action CertificateModule --global --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action CertificateModule --global --actionName nextdescendents
```

read

Usage:

```
am> read CertificateModule --global
```

update

Usage:

```
am> update CertificateModule --global --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "defaults" : {
```

```
     "properties" : {
       "crlHttpParameters" : {
         "title" : "HTTP Parameters for CRL Update",
         "description" : "These parameters will be included in any HTTP CRL call to the Certificate
 Authority<br><br>If the Client or CA certificate contains the Issuing Distribution Point Extension
 then OpenAM will use this information to retrieve the CRL from the distribution point. This property
 allow custom HTTP parameters to be included in the CRL request.<br/><br/>The format of the parameter
 is as follows:<br/><br/><code>param1=value1,param2=value</code>",
         "propertyOrder" : 500,
         "required" : true,
         "type" : "string",
         "exampleValue" : ""
       },
       "cacheCRLsInMemory" : {
         "title" : "Cache CRLs in memory",
         "description" : "The CRLs will be cached in memory",
         "propertyOrder" : 700,
         "required" : true,
         "type" : "boolean",
         "exampleValue" : ""
       },
       "certificateLdapServers" : {
         "title" : "LDAP Server Where Certificates are Stored",
         "description" : "Use this list to set the LDAP server used to search for certificates.
 <br><br>The Certificate authentication module will use this list for the LDAP server used to search
 for certificates. A single entry must be in the format:<br/><br/><code>ldap_server:port</code><br/
><br/>Multiple entries allow associations between OpenAM servers and a LDAP server. The format is:<br/
><br/><code>local server name | server:port</code><br/><br/>The local server name is the full name of
 the server from the list of servers and sites.",
         "propertyOrder" : 1000,
         "required" : true,
         "items" : {
           "type" : "string"
         },
         "type" : "array",
         "exampleValue" : ""
       },
       "trustedRemoteHosts" : {
         "title" : "Trusted Remote Hosts",
         "description" : "A list of IP addresses trusted to supply client certificates.<br><br>If
 SSL/TLS is being terminated at a load balancer or at the Distributed Authentication server then this
 option can be used to ensure that only specified <i>trusted</i> hosts (identified by IP address) are
 allowed to supply client certificates to the certificate module,<br/><br/>Valid values for this list
 are as follows:<ul><li>none</li><li>any</li><li>multiple IP addresses</li></ul><br/><br/>The default
 value of <i>none</i> disables this functionality",
         "propertyOrder" : 1800,
         "required" : true,
         "items" : {
           "type" : "string"
         },
         "type" : "array",
         "exampleValue" : ""
       },
       "matchCertificateInLdap" : {
         "title" : "Match Certificate in LDAP",
         "description" : "The client certificate must exist in the directory for the authentication
 to be successful.",
         "propertyOrder" : 100,
         "required" : true,
```

```
          "type" : "boolean",
          "exampleValue" : ""
        },
        "userBindDN" : {
          "title" : "LDAP Server Authentication User",
          "description" : "DN of the user used by the module to authenticate to the LDAP
 server<br><br>The Certificate module authenticates to the LDAP server in order to search for a
 matching certificate. The DN entered here represents the account used for said authentication and
 must have read/search access to the LDAP server.",
          "propertyOrder" : 1200,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "matchCACertificateToCRL" : {
          "title" : "Match CA Certificate to CRL",
          "description" : "The CA certificate that issued the client certificate will also be checked
 against the CRL.",
          "propertyOrder" : 600,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "iplanet-am-auth-cert-gw-cert-preferred" : {
          "title" : "Use only Certificate from HTTP request header",
          "description" : "Strictly use client cert from HTTP header over cert from HTTPS connection/
servlet attribute",
          "propertyOrder" : 2000,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "certificateAttributeToProfileMapping" : {
          "title" : "Certificate Field Used to Access User Profile",
          "description" : "The certificate module needs to read a value from the client certificate
 that can be used to search the LDAP server for a matching certificate.  ",
          "propertyOrder" : 1500,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "ldapSearchStartDN" : {
          "title" : "LDAP Search Start or Base DN",
          "description" : "The start point in the LDAP server for the certificate search<br><br>When
 entering multiple entries, each entry must be prefixed with a local server name. Multiple entries
 allow different search Base DNs depending on the OpenAM server in use. The format is:<br/><br/
><code>local server name | base dn</code><br/><br/>The local server name is the full name of the
 server from the list of servers and sites.",
          "propertyOrder" : 1100,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "userBindPassword" : {
          "title" : "LDAP Server Authentication Password",
          "description" : "The password for the authentication user",
```

```
          "propertyOrder" : 1300,
          "required" : true,
          "type" : "string",
          "format" : "password",
          "exampleValue" : ""
        },
        "certificateAttributeProfileMappingExtension" : {
          "title" : "SubjectAltNameExt Value Type to Access User Profile",
          "description" : "Use the Subject Alternative Name Field in preference to one of the standard
certificate fields.<br><br>Selecting RFC822Name or UPN will cause this field to have have precedence
over the <i>Certificate Field Used to Access User Profile</i> or <i>Other Certificate Field Used
to Access User Profile</i> attribute.<br/><br/><i>NB </i>The client certificate must contain the
<i>Subject Alternate Name Extension</i> for this function to operate.",
          "propertyOrder" : 1700,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "matchCertificateToCRL" : {
          "title" : "Match Certificate to CRL",
          "description" : "The Client Certificate will be checked against the Certificate Revocation
list held in the directory<br><br>A Certificate Revocation List can be provisioned into the
directory. Having this option enabled will cause all client certificates to be checked against this
list.",
          "propertyOrder" : 300,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "clientCertificateHttpHeaderName" : {
          "title" : "HTTP Header Name for Client Certificate",
          "description" : "The name of the HTTP request header containing the certificate, only used
when <i>Trusted Remote Hosts</i> mode is enabled.",
          "propertyOrder" : 1900,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "otherCertificateAttributeToProfileMapping" : {
          "title" : "Other Certificate Field Used to Access User Profile",
          "description" : "This field is only used if the <i>Certificate Field Used to Access User
Profile</i> attribute is set to <i>other</i>. This field allows a custom certificate field to be used
as the basis of the user search.",
          "propertyOrder" : 1600,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "authenticationLevel" : {
          "title" : "Authentication Level",
          "description" : "The authentication level associated with this module.<br><br>Each
authentication module has an authentication level that can be used to indicate the level of security
associated with the module; 0 is the lowest (and the default).",
          "propertyOrder" : 2100,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "ocspValidationEnabled" : {
```

```
          "title" : "OCSP Validation",
          "description" : "Enable Online Certificate Status Protocol validation for OCSP aware
 certificates<br><br>If the certificate contains OCSP validation information then OpenAM will use this
 information to check the validity of the certificate as part of the authentication process.<br/><br/
><i>NB </i>The OpenAM server must have Internet connectivity for OCSP to work",
          "propertyOrder" : 900,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "crlMatchingCertificateAttribute" : {
          "title" : "Issuer DN Attribute(s) Used to Search LDAP for CRLs",
          "description" : "This is the name of the attribute taken from the CA certificate that will
 be used to search the CRL.<br><br>If only one attribute name is specified, the ldap searchfilter
 will be (attrName=Value_of_the_corresponding_Attribute_from_SubjectDN)<br/>e.g. SubjectDN of issuer
 cert 'C=US, CN=Some CA, serialNumber=123456',attribute name specified is 'CN', searchfilter used
 will be <code>(CN=Some CA)</code><br/><br/>If serveral attribute names are specified, they have
 to separated by <code>,</code>. The resulting ldap searchfilter value will be a comma separated
 list of name attribute values, the search attribute will be <code>cn</code><br/>e.g. SubjectDN of
 issuer cert 'C=US, CN=Some CA, serialNumber=123456',attribute names specified are 'CN,serialNumber',
 searchfilter used will be <code>cn=CN=Some CA,serialNumber=123456</code><br/>The order of the values
 of the attribute names matter as they must match the value of the <code>cn</code> attribute of a
 crlDistributionPoint entry in the directory server.",
          "propertyOrder" : 400,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "updateCRLsFromDistributionPoint" : {
          "title" : "Update CA CRLs from CRLDistributionPoint",
          "description" : "Fetch new CA CRLs from CRLDistributionPoint and update it in
 Directory Server<br><br>If the CA certificate includes an IssuingDistributionPoint or has an
 CRLDistributionPoint extension set OpenAM tries to update the CRLs if neeed (i.e. CRL is out-of-
date). <br/>This property controls if the update should be performed.<br/>This property is only used
 if CA CRL checking is enabled.",
          "propertyOrder" : 800,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "ldapCertificateAttribute" : {
          "title" : "Subject DN Attribute Used to Search LDAP for Certificates",
          "description" : "This is the attribute used to search the directory for the
 certificate<br><br>The Certificate module will search the directory for the certificate using the
 search filter based on this attribute and the value of the Subject DN taken from the certificate.",
          "propertyOrder" : 200,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "sslEnabled" : {
          "title" : "Use SSL/TLS for LDAP Access",
          "description" : "The certificate module will use SSL/TLS to access the LDAP server",
          "propertyOrder" : 1400,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        }
      },
```

```
      "type" : "object",
      "title" : "Realm Defaults"
    }
  }
}
```

CertificateUserExtractorNode

Realm Operations

Resource path: `/realm-config/authentication/authenticationtrees/nodes/product-CertificateUserExtractorNode`

Resource version: `1.0`

create

Usage:

```
am> create CertificateUserExtractorNode --realm Realm --id id --body body
```

Parameters:

`--id`

The unique identifier for the resource.

`--body`

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "certificateAttributeProfileMappingExtension" : {
      "title" : "SubjectAltNameExt Value Type to Access User Profile",
      "description" : "Use the Subject Alternative Name Field in preference to one of the standard
 certificate fields.<br><br>Selecting RFC822Name or UPN will cause this field to have have precedence
 over the <em>Certificate Field Used to Access User Profile</em> or <em>Other Certificate Field Used
 to Access User Profile</em> attribute.",
      "propertyOrder" : 300,
      "type" : "string",
      "exampleValue" : ""
    },
    "otherCertificateAttributeToProfileMapping" : {
      "title" : "Other Certificate Field Used to Access User Profile",
      "description" : "This field is only used if the <em>Certificate Field Used to Access User
 Profile</em> attribute is set to <em>other</em>. This field allows a custom certificate field to be
 used as the basis of the user search.",
      "propertyOrder" : 200,
      "type" : "string",
      "exampleValue" : ""
    },
    "certificateAttributeToProfileMapping" : {
      "title" : "Certificate Field Used to Access User Profile",
      "description" : "The certificate node needs to read a value from the client certificate that can
 be used to search the LDAP server for the user. This value from the certificate will be populated in
 shared state under the username key.",
      "propertyOrder" : 100,
      "type" : "string",
      "exampleValue" : ""
    }
  },
  "required" : [ "certificateAttributeToProfileMapping",
 "certificateAttributeProfileMappingExtension" ]
}
```

delete

Usage:

```
am> delete CertificateUserExtractorNode --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action CertificateUserExtractorNode --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action CertificateUserExtractorNode --realm Realm --actionName getCreatableTypes
```

listOutcomes

List the available outcomes for the node type.

Usage:

```
am> action CertificateUserExtractorNode --realm Realm --body body --actionName listOutcomes
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "title" : "Some configuration of the node. This does not need to be complete against the
 configuration schema."
}
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action CertificateUserExtractorNode --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query CertificateUserExtractorNode --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read CertificateUserExtractorNode --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update CertificateUserExtractorNode --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "certificateAttributeProfileMappingExtension" : {
      "title" : "SubjectAltNameExt Value Type to Access User Profile",
      "description" : "Use the Subject Alternative Name Field in preference to one of the standard
 certificate fields.<br><br>Selecting RFC822Name or UPN will cause this field to have have precedence
 over the <em>Certificate Field Used to Access User Profile</em> or <em>Other Certificate Field Used
 to Access User Profile</em> attribute.",
      "propertyOrder" : 300,
      "type" : "string",
      "exampleValue" : ""
    },
    "otherCertificateAttributeToProfileMapping" : {
      "title" : "Other Certificate Field Used to Access User Profile",
      "description" : "This field is only used if the <em>Certificate Field Used to Access User
 Profile</em> attribute is set to <em>other</em>. This field allows a custom certificate field to be
 used as the basis of the user search.",
      "propertyOrder" : 200,
      "type" : "string",
      "exampleValue" : ""
    },
    "certificateAttributeToProfileMapping" : {
      "title" : "Certificate Field Used to Access User Profile",
      "description" : "The certificate node needs to read a value from the client certificate that can
 be used to search the LDAP server for the user. This value from the certificate will be populated in
 shared state under the username key.",
      "propertyOrder" : 100,
      "type" : "string",
      "exampleValue" : ""
    }
  },
  "required" : [ "certificateAttributeToProfileMapping",
 "certificateAttributeProfileMappingExtension" ]
}
```

CertificateValidationNode

Realm Operations

Resource path: `/realm-config/authentication/authenticationtrees/nodes/product-CertificateValidationNode`

Resource version: `1.0`

create

Usage:

```
am> create CertificateValidationNode --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "userBindDN" : {
      "title" : "LDAP Server Authentication User",
      "description" : "DN of the user used by the node to authenticate to the LDAP server.<br><br>The
Certificate node authenticates to the LDAP server in order to search for a matching certificate. The
DN entered here represents the account used for said authentication and must have read/search access
to the LDAP server.",
      "propertyOrder" : 1200,
      "type" : "string",
      "exampleValue" : ""
    },
    "checkCertificateExpiry" : {
      "title" : "Check Certificate Expiration",
      "description" : "Check to see if the certificate is expired.",
      "propertyOrder" : 200,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "sslEnabled" : {
      "title" : "Use SSL/TLS for LDAP Access",
      "description" : "The certificate node will use SSL/TLS to access the LDAP server.",
      "propertyOrder" : 1400,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "ldapCertificateAttribute" : {
      "title" : "Subject DN Attribute Used to Search LDAP for Certificates",
      "description" : "This is the attribute used to search the directory for the
certificate.<br><br>The Certificate node will search the directory for the certificate using the
search filter based on this attribute and the value of the Subject DN taken from the certificate.",
      "propertyOrder" : 300,
      "type" : "string",
      "exampleValue" : ""
    },
    "cacheCRLsInMemory" : {
      "title" : "Cache CRLs in Memory",
      "description" : "The CRLs will be cached in memory.",
      "propertyOrder" : 700,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "crlMatchingCertificateAttribute" : {
      "title" : "Issuer DN Attribute(s) Used to Search LDAP for CRLs",
      "description" : "This is the name of the attribute taken from the CA certificate that will
be used to search the CRL.<br><br>If only one attribute name is specified, the ldap search filter
will be (attrName=Value_of_the_corresponding_Attribute_from_SubjectDN) e.g. SubjectDN of issuer
cert 'C=US, CN=Some CA, serialNumber=123456',attribute name specified is 'CN', search filter used
```

```
will be <code>(CN=Some CA)</code>.<br><br>If several attribute names are specified, they have
to separated by ,. The resulting ldap search filter value will be a comma separated list of name
attribute values, the search attribute will be cn e.g. SubjectDN of issuer cert 'C=US, CN=Some
CA, serialNumber=123456',attribute names specified are 'CN, serialNumber', search filter used will
be <code>cn=CN=Some CA,serialNumber=123456</code>. The order of the values of the attribute names
matteras they must match the value of the cn attribute of a crlDistributionPoint entry in the
directory server.",
     "propertyOrder" : 500,
     "type" : "string",
     "exampleValue" : ""
   },
   "crlHttpParameters" : {
     "title" : "HTTP Parameters for CRL Update",
     "description" : "These parameters will be included in any HTTP CRL call to the Certificate
Authority.<br><br>If the Client or CA certificate contains the Issuing Distribution Point Extension
then OpenAM will use this information to retrieve the CRL from the distribution point. This property
allow custom HTTP parameters to be included in the CRL request.<br><br>The format of the parameter is
as follows:<br><code>param1=value1,param2=value</code>",
     "propertyOrder" : 600,
     "type" : "string",
     "exampleValue" : ""
   },
   "ldapSearchStartDN" : {
     "title" : "LDAP Search Start or Base DN",
     "description" : "The start point in the LDAP server for the certificate and CRL
search.<br><br>When entering multiple entries, each entry must be prefixed with a local server name.
Multiple entries allow different search Base DNs depending on the OpenAM server in use. The format
is:<br><code>local server name | base dn</code><br><br>The local server name is the full name of the
server from the list of servers and sites.",
     "propertyOrder" : 1100,
     "items" : {
       "type" : "string"
     },
     "type" : "array",
     "exampleValue" : ""
   },
   "ocspValidationEnabled" : {
     "title" : "OCSP Validation",
     "description" : "Enable Online Certificate Status Protocol validation for OCSP aware
certificates.<br><br>If the certificate contains OCSP validation information then OpenAM will
use this information to check thevalidity of the certificate as part of the authentication
process.<br><br>The OpenAM server must have Internet connectivity for OCSP to work.",
     "propertyOrder" : 900,
     "type" : "boolean",
     "exampleValue" : ""
   },
   "matchCertificateInLdap" : {
     "title" : "Match Certificate in LDAP",
     "description" : "The client certificate must exist in the directory for the authentication to be
successful.",
     "propertyOrder" : 100,
     "type" : "boolean",
     "exampleValue" : ""
   },
   "userBindPassword" : {
     "title" : "LDAP Server Authentication Password",
     "description" : "The password for the authentication user.",
     "propertyOrder" : 1300,
     "type" : "string",
```

```
      "format" : "password",
      "exampleValue" : ""
    },
    "matchCertificateToCRL" : {
      "title" : "Match Certificate to CRL",
      "description" : "The Client Certificate will be checked against the Certificate Revocation list
 held in thedirectory.<br><br>A Certificate Revocation List can be provisioned into the directory.
 Having this option enabled will cause all client certificates to be checked against this list.",
      "propertyOrder" : 400,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "updateCRLsFromDistributionPoint" : {
      "title" : "Update CA CRLs from CRLDistributionPoint",
      "description" : "Fetch new CA CRLs from CRLDistributionPoint and update it in Directory
 Server.<br><br>If the CA certificate includes an IssuingDistributionPoint or has an
 CRLDistributionPoint extension set OpenAM tries to update the CRLs if needed (i.e. CRL is out-of-
date).<br>This property controls if the update should be performed.<br>This property is only used if
 CA CRL checking is enabled.",
      "propertyOrder" : 800,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "certificateLdapServers" : {
      "title" : "LDAP Server Where Certificates are Stored",
      "description" : "Use this list to set the LDAP server used to search for
 certificates.<br><br>The Certificate authentication node will use this list for the LDAP server
 used to search for certificates. A single entry must be in the format:<br><code>ldap_server:port</
code><br><br>Multiple entries allow associations between OpenAM servers and a LDAP server. The format
 is:<br><code>local server name | server:port</code><br><br>The local server name is the full name of
 the server from the list of servers and sites.",
      "propertyOrder" : 1000,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    }
  },
  "required" : [ "ldapCertificateAttribute", "updateCRLsFromDistributionPoint",
 "matchCertificateToCRL", "ocspValidationEnabled", "userBindPassword", "cacheCRLsInMemory",
 "sslEnabled", "checkCertificateExpiry", "matchCertificateInLdap", "certificateLdapServers",
 "ldapSearchStartDN", "crlMatchingCertificateAttribute" ]
}
```


delete

Usage:

```
am> delete CertificateValidationNode --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action CertificateValidationNode --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action CertificateValidationNode --realm Realm --actionName getCreatableTypes
```

listOutcomes

List the available outcomes for the node type.

Usage:

```
am> action CertificateValidationNode --realm Realm --body body --actionName listOutcomes
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "title" : "Some configuration of the node. This does not need to be complete against the
 configuration schema."
}
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action CertificateValidationNode --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query CertificateValidationNode --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read CertificateValidationNode --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update CertificateValidationNode --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "userBindDN" : {
      "title" : "LDAP Server Authentication User",
      "description" : "DN of the user used by the node to authenticate to the LDAP server.<br><br>The
 Certificate node authenticates to the LDAP server in order to search for a matching certificate. The
 DN entered here represents the account used for said authentication and must have read/search access
 to the LDAP server.",
      "propertyOrder" : 1200,
      "type" : "string",
      "exampleValue" : ""
    },
    "checkCertificateExpiry" : {
      "title" : "Check Certificate Expiration",
      "description" : "Check to see if the certificate is expired.",
      "propertyOrder" : 200,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "sslEnabled" : {
      "title" : "Use SSL/TLS for LDAP Access",
```

```
      "description" : "The certificate node will use SSL/TLS to access the LDAP server.",
      "propertyOrder" : 1400,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "ldapCertificateAttribute" : {
      "title" : "Subject DN Attribute Used to Search LDAP for Certificates",
      "description" : "This is the attribute used to search the directory for the
certificate.<br><br>The Certificate node will search the directory for the certificate using the
search filter based on this attribute and the value of the Subject DN taken from the certificate.",
      "propertyOrder" : 300,
      "type" : "string",
      "exampleValue" : ""
    },
    "cacheCRLsInMemory" : {
      "title" : "Cache CRLs in Memory",
      "description" : "The CRLs will be cached in memory.",
      "propertyOrder" : 700,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "crlMatchingCertificateAttribute" : {
      "title" : "Issuer DN Attribute(s) Used to Search LDAP for CRLs",
      "description" : "This is the name of the attribute taken from the CA certificate that will
be used to search the CRL.<br><br>If only one attribute name is specified, the ldap search filter
will be (attrName=Value_of_the_corresponding_Attribute_from_SubjectDN) e.g. SubjectDN of issuer
cert 'C=US, CN=Some CA, serialNumber=123456',attribute name specified is 'CN', search filter used
will be <code>(CN=Some CA)</code>.<br><br>If several attribute names are specified, they have
to separated by ,. The resulting ldap search filter value will be a comma separated list of name
attribute values, the search attribute will be cn e.g. SubjectDN of issuer cert 'C=US, CN=Some
CA, serialNumber=123456',attribute names specified are 'CN, serialNumber', search filter used will
be <code>cn=CN=Some CA,serialNumber=123456</code>. The order of the values of the attribute names
matteras they must match the value of the cn attribute of a crlDistributionPoint entry in the
directory server.",
      "propertyOrder" : 500,
      "type" : "string",
      "exampleValue" : ""
    },
    "crlHttpParameters" : {
      "title" : "HTTP Parameters for CRL Update",
      "description" : "These parameters will be included in any HTTP CRL call to the Certificate
Authority.<br><br>If the Client or CA certificate contains the Issuing Distribution Point Extension
then OpenAM will use this information to retrieve the CRL from the distribution point. This property
allow custom HTTP parameters to be included in the CRL request.<br><br>The format of the parameter is
as follows:<br><code>param1=value1,param2=value</code>",
      "propertyOrder" : 600,
      "type" : "string",
      "exampleValue" : ""
    },
    "ldapSearchStartDN" : {
      "title" : "LDAP Search Start or Base DN",
      "description" : "The start point in the LDAP server for the certificate and CRL
search.<br><br>When entering multiple entries, each entry must be prefixed with a local server name.
Multiple entries allow different search Base DNs depending on the OpenAM server in use. The format
is:<br><code>local server name | base dn</code><br><br>The local server name is the full name of the
server from the list of servers and sites.",
      "propertyOrder" : 1100,
      "items" : {
        "type" : "string"
```

```
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "ocspValidationEnabled" : {
      "title" : "OCSP Validation",
      "description" : "Enable Online Certificate Status Protocol validation for OCSP aware
 certificates.<br><br>If the certificate contains OCSP validation information then OpenAM will
 use this information to check thevalidity of the certificate as part of the authentication
 process.<br><br>The OpenAM server must have Internet connectivity for OCSP to work.",
      "propertyOrder" : 900,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "matchCertificateInLdap" : {
      "title" : "Match Certificate in LDAP",
      "description" : "The client certificate must exist in the directory for the authentication to be
 successful.",
      "propertyOrder" : 100,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "userBindPassword" : {
      "title" : "LDAP Server Authentication Password",
      "description" : "The password for the authentication user.",
      "propertyOrder" : 1300,
      "type" : "string",
      "format" : "password",
      "exampleValue" : ""
    },
    "matchCertificateToCRL" : {
      "title" : "Match Certificate to CRL",
      "description" : "The Client Certificate will be checked against the Certificate Revocation list
 held in thedirectory.<br><br>A Certificate Revocation List can be provisioned into the directory.
 Having this option enabled will cause all client certificates to be checked against this list.",
      "propertyOrder" : 400,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "updateCRLsFromDistributionPoint" : {
      "title" : "Update CA CRLs from CRLDistributionPoint",
      "description" : "Fetch new CA CRLs from CRLDistributionPoint and update it in Directory
 Server.<br><br>If the CA certificate includes an IssuingDistributionPoint or has an
 CRLDistributionPoint extension set OpenAM tries to update the CRLs if needed (i.e. CRL is out-of-
date).<br>This property controls if the update should be performed.<br>This property is only used if
 CA CRL checking is enabled.",
      "propertyOrder" : 800,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "certificateLdapServers" : {
      "title" : "LDAP Server Where Certificates are Stored",
      "description" : "Use this list to set the LDAP server used to search for
 certificates.<br><br>The Certificate authentication node will use this list for the LDAP server
 used to search for certificates. A single entry must be in the format:<br><code>ldap_server:port</
code><br><br>Multiple entries allow associations between OpenAM servers and a LDAP server. The format
 is:<br><code>local server name | server:port</code><br><br>The local server name is the full name of
 the server from the list of servers and sites.",
      "propertyOrder" : 1000,
```

```
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    }
  },
  "required" : [ "ldapCertificateAttribute", "updateCRLsFromDistributionPoint",
 "matchCertificateToCRL", "ocspValidationEnabled", "userBindPassword", "cacheCRLsInMemory",
 "sslEnabled", "checkCertificateExpiry", "matchCertificateInLdap", "certificateLdapServers",
 "ldapSearchStartDN", "crlMatchingCertificateAttribute" ]
}
```

ChoiceCollector

Realm Operations

Resource path: `/realm-config/authentication/authenticationtrees/nodes/ChoiceCollectorNode`

Resource version: `1.0`

create

Usage:

```
am> create ChoiceCollector --realm Realm --id id --body body
```

Parameters:

`--id`

The unique identifier for the resource.

`--body`

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "choices" : {
      "title" : "Choices",
      "description" : "List of values that represents the choices for the user.",
      "propertyOrder" : 100,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "defaultChoice" : {
      "title" : "Default Choice",
      "description" : "The default selected choice value.",
      "propertyOrder" : 200,
      "type" : "string",
      "exampleValue" : ""
    },
    "prompt" : {
      "title" : "Prompt",
      "description" : "Prompt displayed on the choice page.",
      "propertyOrder" : 300,
      "type" : "string",
      "exampleValue" : ""
    }
  },
  "required" : [ "prompt", "defaultChoice", "choices" ]
}
```

delete

Usage:

```
am> delete ChoiceCollector --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action ChoiceCollector --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action ChoiceCollector --realm Realm --actionName getCreatableTypes
```

listOutcomes

List the available outcomes for the node type.

Usage:

```
am> action ChoiceCollector --realm Realm --body body --actionName listOutcomes
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "title" : "Some configuration of the node. This does not need to be complete against the
 configuration schema."
}
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action ChoiceCollector --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query ChoiceCollector --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read ChoiceCollector --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update ChoiceCollector --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "choices" : {
      "title" : "Choices",
      "description" : "List of values that represents the choices for the user.",
      "propertyOrder" : 100,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "defaultChoice" : {
      "title" : "Default Choice",
      "description" : "The default selected choice value.",
      "propertyOrder" : 200,
      "type" : "string",
      "exampleValue" : ""
    },
    "prompt" : {
      "title" : "Prompt",
      "description" : "Prompt displayed on the choice page.",
      "propertyOrder" : 300,
      "type" : "string",
      "exampleValue" : ""
    }
  },
  "required" : [ "prompt", "defaultChoice", "choices" ]
}
```

CircleOfTrust

Realm Operations

Resource path: `/realm-config/federation/circlesoftrust`

Resource version: `1.0`

create

Usage:

```
am> create CircleOfTrust --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "description" : {
      "title" : "Description",
      "description" : "",
      "propertyOrder" : 100,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
    },
    "saml2ReaderServiceUrl" : {
      "title" : "SAML2 Reader Service URL",
      "description" : "Location of the SAML2 Reader service that reads the cookie from the Common
 Domain.",
      "propertyOrder" : 500,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
    },
    "status" : {
      "title" : "Status",
      "description" : "",
      "propertyOrder" : 200,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
    },
    "saml2WriterServiceUrl" : {
```

```
      "title" : "SAML2 Writer Service URL",
      "description" : "Location of the SAML2 Writer service that writes the cookie to the Common
 Domain.",
      "propertyOrder" : 400,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
    },
    "trustedProviders" : {
      "title" : "Entity Providers",
      "description" : "Minimum requirements for a circle of trust are one identity provider and one
 service provider.",
      "propertyOrder" : 300,
      "required" : false,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    }
  }
}
```

delete

Usage:

```
am> delete CircleOfTrust --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query CircleOfTrust --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read CircleOfTrust --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update CircleOfTrust --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "description" : {
      "title" : "Description",
      "description" : "",
      "propertyOrder" : 100,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
    },
    "saml2ReaderServiceUrl" : {
      "title" : "SAML2 Reader Service URL",
      "description" : "Location of the SAML2 Reader service that reads the cookie from the Common
 Domain.",
      "propertyOrder" : 500,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
    },
    "status" : {
      "title" : "Status",
      "description" : "",
      "propertyOrder" : 200,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
    },
    "saml2WriterServiceUrl" : {
      "title" : "SAML2 Writer Service URL",
      "description" : "Location of the SAML2 Writer service that writes the cookie to the Common
 Domain.",
```

```
      "propertyOrder" : 400,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
    },
    "trustedProviders" : {
      "title" : "Entity Providers",
      "description" : "Minimum requirements for a circle of trust are one identity provider and one
 service provider.",
      "propertyOrder" : 300,
      "required" : false,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    }
  }
}
```

CommonFederationConfiguration

Global Operations

Resource path: `/global-config/services/federation/common`

Resource version: `1.0`

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action CommonFederationConfiguration --global --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action CommonFederationConfiguration --global --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action CommonFederationConfiguration --global --actionName nextdescendents
```

read

Usage:

```
am> read CommonFederationConfiguration --global
```

update

Usage:

```
am> update CommonFederationConfiguration --global --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "algorithms" : {
      "type" : "object",
      "title" : "Algorithms",
      "propertyOrder" : 2,
      "properties" : {
        "maskGenerationFunction" : {
          "title" : "Mask Generation Function Algorithm",
          "description" : "Which MGF algorithm to use when encrypting the symmetric encryption key
 using RSA OAEP algorithm.",
          "propertyOrder" : 1650,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "QuerySignatureAlgorithmRSA" : {
          "title" : "Query String signature algorithm (RSA)",
          "description" : "The default signature algorithm to use in case of RSA keys.",
          "propertyOrder" : 1300,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "transformationAlgorithm" : {
          "title" : "XML transformation algorithm",
          "description" : "The algorithm used to transform XML documents.",
          "propertyOrder" : 1600,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "rsaKeyTransportAlgorithm" : {
```

```
          "title" : "RSA Key Transport Algorithm",
          "description" : "",
          "propertyOrder" : 1750,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "DigestAlgorithm" : {
          "title" : "XML digest algorithm",
          "description" : "The default digest algorithm to use in signing XML.",
          "propertyOrder" : 1200,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "QuerySignatureAlgorithmDSA" : {
          "title" : "Query String signature algorithm (DSA)",
          "description" : "The default signature algorithm to use in case of DSA keys.",
          "propertyOrder" : 1400,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "aesKeyWrapAlgorithm" : {
          "title" : "AES Key Wrap Algorithm",
          "description" : "Which AES key wrap algorithm to use when the remote entity provider does
not specify which key wrap algorithm it supports.",
          "propertyOrder" : 1700,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "signatureAlgorithm" : {
          "title" : "XML signature algorithm",
          "description" : "The algorithm used to sign XML documents.",
          "propertyOrder" : 1100,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "QuerySignatureAlgorithmEC" : {
          "title" : "Query String signature algorithm (EC)",
          "description" : "The default signature algorithm to use in case of EC keys.",
          "propertyOrder" : 1500,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "canonicalizationAlgorithm" : {
          "title" : "XML canonicalization algorithm",
          "description" : "The algorithm used to canonicalize XML documents.",
          "propertyOrder" : 1000,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "implementationClasses" : {
```

```
    "type" : "object",
    "title" : "Implementation Classes",
    "propertyOrder" : 1,
    "properties" : {
      "loggerClass" : {
        "title" : "Logger SPI implementation class",
        "description" : "The Federation system uses this class to record log entries.<br><br>The
default implementation uses the Logging APIs to record log entries. A custom implementation must
implement the <code>com.sun.identity.plugin.log.Logger</code> interface.",
        "propertyOrder" : 300,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
      },
      "rootUrlProviderClass" : {
        "title" : "Root URL provider SPI implementation class",
        "description" : "The Federation system uses this class to get the root
URL of the AM deployment.<br><br>The default implementation uses the Root URL APIs
to access the OpenAM instance root url. A custom implementation must implement the
<code>org.forgerock.openam.federation.plugin.rooturl.RootUrlProvider</code> interface.",
        "propertyOrder" : 105,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
      },
      "keyProviderClass" : {
        "title" : "KeyProvider SPI implementation class",
        "description" : "The Federation system uses this class to provide access to the
underlying Java keystore.<br><br>The default implementation uses the Java Cryptographic
Engine to provide access to the Java keystore. A custom implementation must implement the
<code>com.sun.identity.saml.xmlsig.KeyProvider</code> interface.",
        "propertyOrder" : 800,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
      },
      "sessionProviderClass" : {
        "title" : "SessionProvider SPI implementation class",
        "description" : "The Federation system uses this class to interface with the
session service.<br><br>The default implementation uses the standard authentication
and SSO APIs to access the session service. A custom implementation must implement the
<code>com.sun.identity.plugin.session.SessionProvider</code> interface.",
        "propertyOrder" : 400,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
      },
      "datastoreClass" : {
        "title" : "Datastore SPI implementation class",
        "description" : "The Federation system uses this class to get/set user
profile attributes.<br><br>The default implementation uses the Identity repository
APIs to access user profile attributes. A custom implementation must implement the
<code>com.sun.identity.plugin.datastore.DataStoreProvider</code> interface.",
        "propertyOrder" : 100,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
      },
      "passwordDecoderClass" : {
```

```
          "title" : "PasswordDecoder SPI implementation class",
          "description" : "The Federation system uses this class to decode password
encoded by OpenAM.<br><br>The default implementation uses the internal OpenAM
decryption API to decode passwords. A custom implementation must implement the
<code>com.sun.identity.saml.xmlsig.PasswordDecoder</code> interface.",
          "propertyOrder" : 600,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "signatureProviderClass" : {
          "title" : "SignatureProvider SPI implementation class",
          "description" : "The Federation system uses this class to digitally sign SAML
documents.<br><br>The default implementation uses the XERCES APIs to sign the documents. A custom
implementation must implement the <code>com.sun.identity.saml.xmlsig.SignatureProvider</code>
interface.",
          "propertyOrder" : 700,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "configurationClass" : {
          "title" : "ConfigurationInstance SPI implementation class",
          "description" : "The Federation system uses this class to fetch
service configuration.<br><br>The default implementation uses the SMS APIs
to access service configuration. A custom implementation must implement the
<code>com.sun.identity.plugin.configuration.ConfigurationInstance</code> interface.",
          "propertyOrder" : 200,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "generalConfig" : {
      "type" : "object",
      "title" : "General Configuration",
      "propertyOrder" : 0,
      "properties" : {
        "samlErrorPageUrl" : {
          "title" : "SAML Error Page URL",
          "description" : "OpenAM redirects users here when an error occurs in the SAML2
engine.<br><br>Both relative and absolute URLs are supported. Users are redirected to an absolute URL
using the configured HTTP Binding whereas relative URLs are displayed within the request.",
          "propertyOrder" : 1700,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "samlErrorPageHttpBinding" : {
          "title" : "SAML Error Page HTTP Binding",
          "description" : "The possible values are HTTP-Redirect or HTTP-POST.",
          "propertyOrder" : 1800,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "maxContentLength" : {
          "title" : "Maximum allowed content length",
```

```
          "description" : "The maximum content length allowed in federation communications, in
 bytes.",
          "propertyOrder" : 500,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "certificateChecking" : {
          "title" : "Check presence of certificates",
          "description" : "Enable checking of certificates against local copy<br><br>Whether to verify
 that the partner's signing certificate included in the Federation XML document is the same as the one
 stored in the said partner's meta data.",
          "propertyOrder" : 900,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "montoring" : {
      "type" : "object",
      "title" : "Monitoring",
      "propertyOrder" : 3,
      "properties" : {
        "monitoringAgentClass" : {
          "title" : "Monitoring Agent Provider Class",
          "description" : "The Federation system uses this class to gain access to the monitoring
 system.<br><br>The default implementation uses the built-in OpenAM monitoring system. A custom
 implementation must implement the <code>com.sun.identity.plugin.monitoring.FedMonAgent</code>
 interface.",
          "propertyOrder" : 1900,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "monitoringSaml2Class" : {
          "title" : "Monitoring Provider Class for SAML2",
          "description" : "The SAML2 engine uses this class to gain access to the monitoring
 system.<br><br>The default implementation uses the built-in OpenAM monitoring system. A custom
 implementation must implement the <code>com.sun.identity.plugin.monitoring.FedMonSAML2Svc</code>
 interface.",
          "propertyOrder" : 2100,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    }
  }
}
```

ConditionTypes

Realm Operations

Service for querying and reading the environment condition types stored in OpenAM. Environment condition types describe the JSON representation of environment conditions that you can use in policy definitions

Resource path: `/conditiontypes`

Resource version: `1.0`

query

Query the list of environment condition types

Usage:

```
am> query ConditionTypes --realm Realm --filter filter
```

Parameters:

`--filter`

A CREST formatted query filter, where "true" will query all. Fields that can be queried: [*]

read

Read an individual environment condition type by providing the unique identifier title

Usage:

```
am> read ConditionTypes --realm Realm --id id
```

Parameters:

`--id`

The unique identifier for the resource.

ConfigurationVersionService

Global Operations

Resource path: `/global-config/services/ConfigurationVersionService`

Resource version: `1.0`

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action ConfigurationVersionService --global --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action ConfigurationVersionService --global --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action ConfigurationVersionService --global --actionName nextdescendents
```

read

Usage:

```
am> read ConfigurationVersionService --global
```

update

Usage:

```
am> update ConfigurationVersionService --global --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "configurationVersion" : {
      "title" : "Configuration Version",
      "description" : "AM's configuration version",
      "propertyOrder" : null,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
```

ConsentCollector

Realm Operations

Resource path: `/realm-config/authentication/authenticationtrees/nodes/ConsentNode`

Resource version: `1.0`

create

Usage:

```
am> create ConsentCollector --realm Realm --id id --body body
```

Parameters:

`--id`

The unique identifier for the resource.

`--body`

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "allRequired" : {
      "title" : "All Mappings Required",
      "description" : "All mappings listed by this node require consent in order to move forward.",
      "propertyOrder" : 100,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "message" : {
      "title" : "Privacy & Consent Message",
      "description" : "Localised message providing the privacy and consent notice.",
      "propertyOrder" : 200,
      "patternProperties" : {
        ".*" : {
          "type" : "string"
        }
      },
      "type" : "object",
      "exampleValue" : ""
    }
  },
  "required" : [ "message", "allRequired" ]
}
```

delete

Usage:

```
am> delete ConsentCollector --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action ConsentCollector --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action ConsentCollector --realm Realm --actionName getCreatableTypes
```

listOutcomes

List the available outcomes for the node type.

Usage:

```
am> action ConsentCollector --realm Realm --body body --actionName listOutcomes
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "title" : "Some configuration of the node. This does not need to be complete against the
 configuration schema."
}
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action ConsentCollector --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query ConsentCollector --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read ConsentCollector --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update ConsentCollector --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "allRequired" : {
      "title" : "All Mappings Required",
      "description" : "All mappings listed by this node require consent in order to move forward.",
      "propertyOrder" : 100,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "message" : {
      "title" : "Privacy & Consent Message",
      "description" : "Localised message providing the privacy and consent notice.",
      "propertyOrder" : 200,
      "patternProperties" : {
        ".*" : {
          "type" : "string"
        }
      },
      "type" : "object",
      "exampleValue" : ""
    }
  },
  "required" : [ "message", "allRequired" ]
}
```

CookiePresenceDecisionNode

Realm Operations

Resource path: `/realm-config/authentication/authenticationtrees/nodes/CookiePresenceDecisionNode`

Resource version: `1.0`

create

Usage:

```
am> create CookiePresenceDecisionNode --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "cookieName" : {
      "title" : "Name of Cookie",
      "description" : "",
      "propertyOrder" : 100,
      "type" : "string",
      "exampleValue" : ""
    }
  },
  "required" : [ "cookieName" ]
}
```

delete

Usage:

```
am> delete CookiePresenceDecisionNode --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action CookiePresenceDecisionNode --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action CookiePresenceDecisionNode --realm Realm --actionName getCreatableTypes
```

listOutcomes

List the available outcomes for the node type.

Usage:

```
am> action CookiePresenceDecisionNode --realm Realm --body body --actionName listOutcomes
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "title" : "Some configuration of the node. This does not need to be complete against the
 configuration schema."
}
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action CookiePresenceDecisionNode --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query CookiePresenceDecisionNode --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read CookiePresenceDecisionNode --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update CookiePresenceDecisionNode --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "cookieName" : {
      "title" : "Name of Cookie",
      "description" : "",
      "propertyOrder" : 100,
      "type" : "string",
      "exampleValue" : ""
    }
  },
  "required" : [ "cookieName" ]
}
```

CorsConfiguration

Global Operations

Resource path: `/global-config/services/CorsService/configuration`

Resource version: `1.0`

create

Usage:

```
am> create CorsConfiguration --global --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "exposedHeaders" : {
      "title" : "Exposed Headers",
      "description" : "The set of headers to transmit in the header Access-Control-Expose-Headers.",
      "propertyOrder" : 40,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "enabled" : {
      "title" : "Enable the CORS filter",
      "description" : "If disable, no CORS headers will be added to responses.",
      "propertyOrder" : 2,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "acceptedMethods" : {
      "title" : "Accepted Methods",
      "description" : "The set of (non-simple) accepted methods, included in the pre-flight response
 in the header Access-Control-Allow-Methods.",
      "propertyOrder" : 20,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
```

```
    "allowCredentials" : {
      "title" : "Allow Credentials",
      "description" : "Whether to transmit the Access-Control-Allow-Credentials: true header in the
 response.",
      "propertyOrder" : 60,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "acceptedHeaders" : {
      "title" : "Accepted Headers",
      "description" : "The set of (non-simple) accepted headers, included in the pre-flight response
 in the header Access-Control-Allow-Headers.",
      "propertyOrder" : 30,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "maxAge" : {
      "title" : "Max Age",
      "description" : "The max age (in seconds) for caching, included in the pre-flight response in
 the header Access-Control-Max-Age.",
      "propertyOrder" : 50,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "acceptedOrigins" : {
      "title" : "Accepted Origins",
      "description" : "The set of accepted origins.",
      "propertyOrder" : 10,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    }
  }
}
```

delete

Usage:

```
am> delete CorsConfiguration --global --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action CorsConfiguration --global --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action CorsConfiguration --global --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action CorsConfiguration --global --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query CorsConfiguration --global --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read CorsConfiguration --global --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update CorsConfiguration --global --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "exposedHeaders" : {
      "title" : "Exposed Headers",
      "description" : "The set of headers to transmit in the header Access-Control-Expose-Headers.",
      "propertyOrder" : 40,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "enabled" : {
      "title" : "Enable the CORS filter",
      "description" : "If disable, no CORS headers will be added to responses.",
      "propertyOrder" : 2,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "acceptedMethods" : {
      "title" : "Accepted Methods",
      "description" : "The set of (non-simple) accepted methods, included in the pre-flight response
 in the header Access-Control-Allow-Methods.",
      "propertyOrder" : 20,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "allowCredentials" : {
      "title" : "Allow Credentials",
      "description" : "Whether to transmit the Access-Control-Allow-Credentials: true header in the
 response.",
      "propertyOrder" : 60,
      "required" : true,
      "type" : "boolean",
```

```
      "exampleValue" : ""
    },
    "acceptedHeaders" : {
      "title" : "Accepted Headers",
      "description" : "The set of (non-simple) accepted headers, included in the pre-flight response
 in the header Access-Control-Allow-Headers.",
      "propertyOrder" : 30,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "maxAge" : {
      "title" : "Max Age",
      "description" : "The max age (in seconds) for caching, included in the pre-flight response in
 the header Access-Control-Max-Age.",
      "propertyOrder" : 50,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "acceptedOrigins" : {
      "title" : "Accepted Origins",
      "description" : "The set of accepted origins.",
      "propertyOrder" : 10,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    }
  }
}
```

CreateObject

Realm Operations

Resource path: `/realm-config/authentication/authenticationtrees/nodes/CreateObjectNode`

Resource version: `1.0`

create

Usage:

```
am> create CreateObject --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "identityResource" : {
      "title" : "Identity Resource",
      "description" : "The identity resource in IDM that this node will create. This is used to aid
 node input requirement declaration.  Must match identity resource of the current tree.",
      "propertyOrder" : 100,
      "type" : "string",
      "exampleValue" : ""
    }
  },
  "required" : [ "identityResource" ]
}
```

delete

Usage:

```
am> delete CreateObject --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action CreateObject --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action CreateObject --realm Realm --actionName getCreatableTypes
```

listOutcomes

List the available outcomes for the node type.

Usage:

```
am> action CreateObject --realm Realm --body body --actionName listOutcomes
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "title" : "Some configuration of the node. This does not need to be complete against the
 configuration schema."
}
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action CreateObject --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query CreateObject --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read CreateObject --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update CreateObject --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "identityResource" : {
      "title" : "Identity Resource",
      "description" : "The identity resource in IDM that this node will create. This is used to aid
 node input requirement declaration.  Must match identity resource of the current tree.",
      "propertyOrder" : 100,
      "type" : "string",
      "exampleValue" : ""
    }
  },
  "required" : [ "identityResource" ]
}
```

CreatePassword

Realm Operations

Resource path: `/realm-config/authentication/authenticationtrees/nodes/CreatePasswordNode`

Resource version: `1.0`

create

Usage:

```
am> create CreatePassword --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "minPasswordLength" : {
      "title" : "minPasswordLength",
      "description" : "",
      "propertyOrder" : 100,
      "type" : "integer",
      "exampleValue" : ""
    }
  },
  "required" : [ "minPasswordLength" ]
}
```

delete

Usage:

```
am> delete CreatePassword --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action CreatePassword --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action CreatePassword --realm Realm --actionName getCreatableTypes
```

listOutcomes

List the available outcomes for the node type.

Usage:

```
am> action CreatePassword --realm Realm --body body --actionName listOutcomes
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "title" : "Some configuration of the node. This does not need to be complete against the
 configuration schema."
}
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action CreatePassword --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query CreatePassword --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read CreatePassword --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update CreatePassword --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "minPasswordLength" : {
      "title" : "minPasswordLength",
      "description" : "",
      "propertyOrder" : 100,
      "type" : "integer",
      "exampleValue" : ""
    }
  },
  "required" : [ "minPasswordLength" ]
}
```

Csv

Realm Operations

Resource path: `/realm-config/services/audit/CSV`

Resource version: `1.0`

create

Usage:

```
am> create Csv --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "csvFileRetention" : {
      "type" : "object",
      "title" : "File Retention",
      "propertyOrder" : 4,
      "properties" : {
        "retentionMinFreeSpaceRequired" : {
          "title" : "Minimum Free Space Required",
          "description" : "Minimum amount of disk space required, in bytes, on the system where audit
 files are stored. A negative or zero value indicates this policy is disabled.",
          "propertyOrder" : 1400,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "retentionMaxNumberOfHistoryFiles" : {
          "title" : "Maximum Number of Historical Files",
          "description" : "Maximum number of backup audit files allowed. A value of <code>-1</code>
 disables pruning of old history files.",
          "propertyOrder" : 1200,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "retentionMaxDiskSpaceToUse" : {
          "title" : "Maximum Disk Space",
          "description" : "The maximum amount of disk space the audit files can occupy, in bytes. A
 negative or zero value indicates this policy is disabled.",
          "propertyOrder" : 1300,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "csvFileRotation" : {
      "type" : "object",
      "title" : "File Rotation",
      "propertyOrder" : 3,
      "properties" : {
        "rotationInterval" : {
          "title" : "Rotation Interval",
          "description" : "Interval to trigger audit file rotations, in seconds. A negative or zero
 value disables this feature.",
          "propertyOrder" : 1000,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "rotationTimes" : {
          "title" : "Rotation Times",
          "description" : "Durations after midnight to trigger file rotation, in seconds.",
          "propertyOrder" : 1100,
```

```
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "rotationMaxFileSize" : {
          "title" : "Maximum File Size",
          "description" : "Maximum size, in bytes, which an audit file can grow to before rotation is
triggered. A negative or zero value indicates this policy is disabled.",
          "propertyOrder" : 700,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "rotationFilePrefix" : {
          "title" : "File Rotation Prefix",
          "description" : "Prefix to prepend to audit files when rotating audit files.",
          "propertyOrder" : 800,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "rotationEnabled" : {
          "title" : "Rotation Enabled",
          "description" : "Enables and disables audit file rotation.",
          "propertyOrder" : 600,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "rotationFileSuffix" : {
          "title" : "File Rotation Suffix",
          "description" : "Suffix to append to audit files when they are rotated. Suffix should be a
timestamp.",
          "propertyOrder" : 900,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "csvBuffering" : {
      "type" : "object",
      "title" : "Buffering",
      "propertyOrder" : 5,
      "properties" : {
        "bufferingEnabled" : {
          "title" : "Buffering Enabled",
          "description" : "Enables or disables buffering.",
          "propertyOrder" : 1500,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "bufferingAutoFlush" : {
          "title" : "Flush Each Event Immediately",
```

```
          "description" : "Performance may be improved by writing all buffered events before
flushing.",
          "propertyOrder" : 1600,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        }
      }
    },
    "csvConfig" : {
      "type" : "object",
      "title" : "CSV Configuration",
      "propertyOrder" : 2,
      "properties" : {
        "location" : {
          "title" : "Log Directory",
          "description" : "Directory in which to store audit log CSV files.",
          "propertyOrder" : 500,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "commonHandler" : {
      "type" : "object",
      "title" : "General Handler Configuration",
      "propertyOrder" : 0,
      "properties" : {
        "topics" : {
          "title" : "Topics",
          "description" : "List of topics handled by an audit event handler.",
          "propertyOrder" : 400,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "enabled" : {
          "title" : "Enabled",
          "description" : "Enables or disables an audit event handler.",
          "propertyOrder" : 300,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        }
      }
    },
    "csvSecurity" : {
      "type" : "object",
      "title" : "Tamper Evident Configuration",
      "propertyOrder" : 6,
      "properties" : {
        "securitySignatureInterval" : {
          "title" : "Signature Interval",
          "description" : "Signature generation interval, in seconds.",
          "propertyOrder" : 2000,
```

```
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "securityEnabled" : {
          "title" : "Is Enabled",
          "description" : "Enables the CSV tamper evident feature.",
          "propertyOrder" : 1700,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "securityPassword" : {
          "title" : "Certificate Store Password",
          "description" : "Password for Java keystore.",
          "propertyOrder" : 1900,
          "required" : false,
          "type" : "string",
          "format" : "password",
          "exampleValue" : ""
        },
        "securityFilename" : {
          "title" : "Certificate Store Location",
          "description" : "Path to Java keystore.",
          "propertyOrder" : 1800,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "commonHandlerPlugin" : {
      "type" : "object",
      "title" : "Audit Event Handler Factory",
      "propertyOrder" : 1,
      "properties" : {
        "handlerFactory" : {
          "title" : "Factory Class Name",
          "description" : "The fully qualified class name of the factory
 responsible for creating the Audit Event Handler. The class must implement
 <code>org.forgerock.openam.audit.AuditEventHandlerFactory</code>.",
          "propertyOrder" : 2100,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    }
  }
}
```

delete

Usage:

```
am> delete Csv --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action Csv --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action Csv --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action Csv --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query Csv --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read Csv --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update Csv --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "csvFileRetention" : {
      "type" : "object",
      "title" : "File Retention",
      "propertyOrder" : 4,
      "properties" : {
        "retentionMinFreeSpaceRequired" : {
          "title" : "Minimum Free Space Required",
          "description" : "Minimum amount of disk space required, in bytes, on the system where audit
 files are stored. A negative or zero value indicates this policy is disabled.",
          "propertyOrder" : 1400,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "retentionMaxNumberOfHistoryFiles" : {
          "title" : "Maximum Number of Historical Files",
          "description" : "Maximum number of backup audit files allowed. A value of <code>-1</code>
 disables pruning of old history files.",
          "propertyOrder" : 1200,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "retentionMaxDiskSpaceToUse" : {
          "title" : "Maximum Disk Space",
          "description" : "The maximum amount of disk space the audit files can occupy, in bytes. A
 negative or zero value indicates this policy is disabled.",
          "propertyOrder" : 1300,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
```

```
      }
    }
  },
  "csvFileRotation" : {
    "type" : "object",
    "title" : "File Rotation",
    "propertyOrder" : 3,
    "properties" : {
      "rotationInterval" : {
        "title" : "Rotation Interval",
        "description" : "Interval to trigger audit file rotations, in seconds. A negative or zero
value disables this feature.",
        "propertyOrder" : 1000,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
      },
      "rotationTimes" : {
        "title" : "Rotation Times",
        "description" : "Durations after midnight to trigger file rotation, in seconds.",
        "propertyOrder" : 1100,
        "required" : true,
        "items" : {
          "type" : "string"
        },
        "type" : "array",
        "exampleValue" : ""
      },
      "rotationMaxFileSize" : {
        "title" : "Maximum File Size",
        "description" : "Maximum size, in bytes, which an audit file can grow to before rotation is
triggered. A negative or zero value indicates this policy is disabled.",
        "propertyOrder" : 700,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
      },
      "rotationFilePrefix" : {
        "title" : "File Rotation Prefix",
        "description" : "Prefix to prepend to audit files when rotating audit files.",
        "propertyOrder" : 800,
        "required" : false,
        "type" : "string",
        "exampleValue" : ""
      },
      "rotationEnabled" : {
        "title" : "Rotation Enabled",
        "description" : "Enables and disables audit file rotation.",
        "propertyOrder" : 600,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
      },
      "rotationFileSuffix" : {
        "title" : "File Rotation Suffix",
        "description" : "Suffix to append to audit files when they are rotated. Suffix should be a
timestamp.",
        "propertyOrder" : 900,
        "required" : false,
```

```
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "csvBuffering" : {
      "type" : "object",
      "title" : "Buffering",
      "propertyOrder" : 5,
      "properties" : {
        "bufferingEnabled" : {
          "title" : "Buffering Enabled",
          "description" : "Enables or disables buffering.",
          "propertyOrder" : 1500,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "bufferingAutoFlush" : {
          "title" : "Flush Each Event Immediately",
          "description" : "Performance may be improved by writing all buffered events before
flushing.",
          "propertyOrder" : 1600,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        }
      }
    },
    "csvConfig" : {
      "type" : "object",
      "title" : "CSV Configuration",
      "propertyOrder" : 2,
      "properties" : {
        "location" : {
          "title" : "Log Directory",
          "description" : "Directory in which to store audit log CSV files.",
          "propertyOrder" : 500,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "commonHandler" : {
      "type" : "object",
      "title" : "General Handler Configuration",
      "propertyOrder" : 0,
      "properties" : {
        "topics" : {
          "title" : "Topics",
          "description" : "List of topics handled by an audit event handler.",
          "propertyOrder" : 400,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
```

```
        },
        "enabled" : {
          "title" : "Enabled",
          "description" : "Enables or disables an audit event handler.",
          "propertyOrder" : 300,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        }
      }
    },
    "csvSecurity" : {
      "type" : "object",
      "title" : "Tamper Evident Configuration",
      "propertyOrder" : 6,
      "properties" : {
        "securitySignatureInterval" : {
          "title" : "Signature Interval",
          "description" : "Signature generation interval, in seconds.",
          "propertyOrder" : 2000,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "securityEnabled" : {
          "title" : "Is Enabled",
          "description" : "Enables the CSV tamper evident feature.",
          "propertyOrder" : 1700,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "securityPassword" : {
          "title" : "Certificate Store Password",
          "description" : "Password for Java keystore.",
          "propertyOrder" : 1900,
          "required" : false,
          "type" : "string",
          "format" : "password",
          "exampleValue" : ""
        },
        "securityFilename" : {
          "title" : "Certificate Store Location",
          "description" : "Path to Java keystore.",
          "propertyOrder" : 1800,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "commonHandlerPlugin" : {
      "type" : "object",
      "title" : "Audit Event Handler Factory",
      "propertyOrder" : 1,
      "properties" : {
        "handlerFactory" : {
          "title" : "Factory Class Name",
```

```
          "description" : "The fully qualified class name of the factory
 responsible for creating the Audit Event Handler. The class must implement
 <code>org.forgerock.openam.audit.AuditEventHandlerFactory</code>.",
          "propertyOrder" : 2100,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    }
  }
}
```

Global Operations

Resource path: `/global-config/services/audit/CSV`

Resource version: `1.0`

create

Usage:

```
am> create Csv --global --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "csvFileRetention" : {
      "type" : "object",
      "title" : "File Retention",
      "propertyOrder" : 4,
      "properties" : {
        "retentionMinFreeSpaceRequired" : {
          "title" : "Minimum Free Space Required",
          "description" : "Minimum amount of disk space required, in bytes, on the system where audit
 files are stored. A negative or zero value indicates this policy is disabled.",
          "propertyOrder" : 1400,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "retentionMaxNumberOfHistoryFiles" : {
          "title" : "Maximum Number of Historical Files",
```

```
          "description" : "Maximum number of backup audit files allowed. A value of <code>-1</code>
disables pruning of old history files.",
          "propertyOrder" : 1200,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "retentionMaxDiskSpaceToUse" : {
          "title" : "Maximum Disk Space",
          "description" : "The maximum amount of disk space the audit files can occupy, in bytes. A
negative or zero value indicates this policy is disabled.",
          "propertyOrder" : 1300,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "commonHandler" : {
      "type" : "object",
      "title" : "General Handler Configuration",
      "propertyOrder" : 0,
      "properties" : {
        "enabled" : {
          "title" : "Enabled",
          "description" : "Enables or disables an audit event handler.",
          "propertyOrder" : 300,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "topics" : {
          "title" : "Topics",
          "description" : "List of topics handled by an audit event handler.",
          "propertyOrder" : 400,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        }
      }
    },
    "csvFileRotation" : {
      "type" : "object",
      "title" : "File Rotation",
      "propertyOrder" : 3,
      "properties" : {
        "rotationInterval" : {
          "title" : "Rotation Interval",
          "description" : "Interval to trigger audit file rotations, in seconds. A negative or zero
value disables this feature.",
          "propertyOrder" : 1000,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "rotationTimes" : {
```

```
          "title" : "Rotation Times",
          "description" : "Durations after midnight to trigger file rotation, in seconds.",
          "propertyOrder" : 1100,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "rotationFileSuffix" : {
          "title" : "File Rotation Suffix",
          "description" : "Suffix to append to audit files when they are rotated. Suffix should be a
timestamp.",
          "propertyOrder" : 900,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "rotationMaxFileSize" : {
          "title" : "Maximum File Size",
          "description" : "Maximum size, in bytes, which an audit file can grow to before rotation is
triggered. A negative or zero value indicates this policy is disabled.",
          "propertyOrder" : 700,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "rotationEnabled" : {
          "title" : "Rotation Enabled",
          "description" : "Enables and disables audit file rotation.",
          "propertyOrder" : 600,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "rotationFilePrefix" : {
          "title" : "File Rotation Prefix",
          "description" : "Prefix to prepend to audit files when rotating audit files.",
          "propertyOrder" : 800,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "commonHandlerPlugin" : {
      "type" : "object",
      "title" : "Audit Event Handler Factory",
      "propertyOrder" : 1,
      "properties" : {
        "handlerFactory" : {
          "title" : "Factory Class Name",
          "description" : "The fully qualified class name of the factory
responsible for creating the Audit Event Handler. The class must implement
<code>org.forgerock.openam.audit.AuditEventHandlerFactory</code>.",
          "propertyOrder" : 2100,
          "required" : true,
          "type" : "string",
```

```
          "exampleValue" : ""
        }
      }
    },
    "csvSecurity" : {
      "type" : "object",
      "title" : "Tamper Evident Configuration",
      "propertyOrder" : 6,
      "properties" : {
        "securityFilename" : {
          "title" : "Certificate Store Location",
          "description" : "Path to Java keystore.",
          "propertyOrder" : 1800,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "securitySignatureInterval" : {
          "title" : "Signature Interval",
          "description" : "Signature generation interval, in seconds.",
          "propertyOrder" : 2000,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "securityEnabled" : {
          "title" : "Is Enabled",
          "description" : "Enables the CSV tamper evident feature.",
          "propertyOrder" : 1700,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "securityPassword" : {
          "title" : "Certificate Store Password",
          "description" : "Password for Java keystore.",
          "propertyOrder" : 1900,
          "required" : false,
          "type" : "string",
          "format" : "password",
          "exampleValue" : ""
        }
      }
    },
    "csvBuffering" : {
      "type" : "object",
      "title" : "Buffering",
      "propertyOrder" : 5,
      "properties" : {
        "bufferingEnabled" : {
          "title" : "Buffering Enabled",
          "description" : "Enables or disables buffering.",
          "propertyOrder" : 1500,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "bufferingAutoFlush" : {
          "title" : "Flush Each Event Immediately",
```

```
          "description" : "Performance may be improved by writing all buffered events before
 flushing.",
          "propertyOrder" : 1600,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        }
      }
    },
    "csvConfig" : {
      "type" : "object",
      "title" : "CSV Configuration",
      "propertyOrder" : 2,
      "properties" : {
        "location" : {
          "title" : "Log Directory",
          "description" : "Directory in which to store audit log CSV files.",
          "propertyOrder" : 500,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    }
  }
}
```

delete

Usage:

```
am> delete Csv --global --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action Csv --global --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action Csv --global --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action Csv --global --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query Csv --global --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read Csv --global --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update Csv --global --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "csvFileRetention" : {
      "type" : "object",
      "title" : "File Retention",
      "propertyOrder" : 4,
      "properties" : {
        "retentionMinFreeSpaceRequired" : {
          "title" : "Minimum Free Space Required",
          "description" : "Minimum amount of disk space required, in bytes, on the system where audit
 files are stored. A negative or zero value indicates this policy is disabled.",
          "propertyOrder" : 1400,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "retentionMaxNumberOfHistoryFiles" : {
          "title" : "Maximum Number of Historical Files",
          "description" : "Maximum number of backup audit files allowed. A value of <code>-1</code>
 disables pruning of old history files.",
          "propertyOrder" : 1200,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "retentionMaxDiskSpaceToUse" : {
          "title" : "Maximum Disk Space",
          "description" : "The maximum amount of disk space the audit files can occupy, in bytes. A
 negative or zero value indicates this policy is disabled.",
          "propertyOrder" : 1300,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "commonHandler" : {
      "type" : "object",
      "title" : "General Handler Configuration",
      "propertyOrder" : 0,
      "properties" : {
        "enabled" : {
          "title" : "Enabled",
          "description" : "Enables or disables an audit event handler.",
          "propertyOrder" : 300,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "topics" : {
          "title" : "Topics",
          "description" : "List of topics handled by an audit event handler.",
          "propertyOrder" : 400,
          "required" : true,
```

```
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        }
      }
    },
    "csvFileRotation" : {
      "type" : "object",
      "title" : "File Rotation",
      "propertyOrder" : 3,
      "properties" : {
        "rotationInterval" : {
          "title" : "Rotation Interval",
          "description" : "Interval to trigger audit file rotations, in seconds. A negative or zero
value disables this feature.",
          "propertyOrder" : 1000,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "rotationTimes" : {
          "title" : "Rotation Times",
          "description" : "Durations after midnight to trigger file rotation, in seconds.",
          "propertyOrder" : 1100,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "rotationFileSuffix" : {
          "title" : "File Rotation Suffix",
          "description" : "Suffix to append to audit files when they are rotated. Suffix should be a
timestamp.",
          "propertyOrder" : 900,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "rotationMaxFileSize" : {
          "title" : "Maximum File Size",
          "description" : "Maximum size, in bytes, which an audit file can grow to before rotation is
triggered. A negative or zero value indicates this policy is disabled.",
          "propertyOrder" : 700,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "rotationEnabled" : {
          "title" : "Rotation Enabled",
          "description" : "Enables and disables audit file rotation.",
          "propertyOrder" : 600,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
```

```
        "rotationFilePrefix" : {
          "title" : "File Rotation Prefix",
          "description" : "Prefix to prepend to audit files when rotating audit files.",
          "propertyOrder" : 800,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "commonHandlerPlugin" : {
      "type" : "object",
      "title" : "Audit Event Handler Factory",
      "propertyOrder" : 1,
      "properties" : {
        "handlerFactory" : {
          "title" : "Factory Class Name",
          "description" : "The fully qualified class name of the factory
responsible for creating the Audit Event Handler. The class must implement
<code>org.forgerock.openam.audit.AuditEventHandlerFactory</code>.",
          "propertyOrder" : 2100,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "csvSecurity" : {
      "type" : "object",
      "title" : "Tamper Evident Configuration",
      "propertyOrder" : 6,
      "properties" : {
        "securityFilename" : {
          "title" : "Certificate Store Location",
          "description" : "Path to Java keystore.",
          "propertyOrder" : 1800,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "securitySignatureInterval" : {
          "title" : "Signature Interval",
          "description" : "Signature generation interval, in seconds.",
          "propertyOrder" : 2000,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "securityEnabled" : {
          "title" : "Is Enabled",
          "description" : "Enables the CSV tamper evident feature.",
          "propertyOrder" : 1700,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "securityPassword" : {
          "title" : "Certificate Store Password",
          "description" : "Password for Java keystore.",
```

```
          "propertyOrder" : 1900,
          "required" : false,
          "type" : "string",
          "format" : "password",
          "exampleValue" : ""
        }
      }
    },
    "csvBuffering" : {
      "type" : "object",
      "title" : "Buffering",
      "propertyOrder" : 5,
      "properties" : {
        "bufferingEnabled" : {
          "title" : "Buffering Enabled",
          "description" : "Enables or disables buffering.",
          "propertyOrder" : 1500,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "bufferingAutoFlush" : {
          "title" : "Flush Each Event Immediately",
          "description" : "Performance may be improved by writing all buffered events before
 flushing.",
          "propertyOrder" : 1600,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        }
      }
    },
    "csvConfig" : {
      "type" : "object",
      "title" : "CSV Configuration",
      "propertyOrder" : 2,
      "properties" : {
        "location" : {
          "title" : "Log Directory",
          "description" : "Directory in which to store audit log CSV files.",
          "propertyOrder" : 500,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    }
  }
}
```

CtsDataStoreProperties

Global Operations

An object of property key-value pairs

Resource path: `/global-config/servers/{serverName}/properties/cts`

Resource version: `1.0`

read

Usage:

```
am> read CtsDataStoreProperties --global --serverName serverName
```

Parameters:

`--serverName`

An object of property key-value pairs

update

Usage:

```
am> update CtsDataStoreProperties --global --serverName serverName --body body
```

Parameters:

`--serverName`

An object of property key-value pairs

`--body`

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "amconfig.org.forgerock.services.cts.store.common.section" : {
      "title" : "CTS Token Store",
      "type" : "object",
      "propertyOrder" : 0,
      "properties" : {
        "org.forgerock.services.cts.store.location" : {
          "title" : "Store Mode",
          "type" : "object",
          "propertyOrder" : 0,
          "description" : "",
```

```
          "properties" : {
            "value" : {
              "enum" : [ "default", "external" ],
              "options" : {
                "enum_titles" : [ "Default Token Store", "External Token Store" ]
              },
              "type" : "string",
              "required" : false
            },
            "inherited" : {
              "type" : "boolean",
              "required" : true
            }
          }
        },
        "org.forgerock.services.cts.store.root.suffix" : {
          "title" : "Root Suffix",
          "type" : "object",
          "propertyOrder" : 1,
          "description" : "",
          "properties" : {
            "value" : {
              "type" : "string",
              "required" : false
            },
            "inherited" : {
              "type" : "boolean",
              "required" : true
            }
          }
        },
        "org.forgerock.services.cts.store.max.connections" : {
          "title" : "Max Connections",
          "type" : "object",
          "propertyOrder" : 2,
          "description" : "",
          "properties" : {
            "value" : {
              "type" : "string",
              "required" : false
            },
            "inherited" : {
              "type" : "boolean",
              "required" : true
            }
          }
        },
        "org.forgerock.services.cts.store.page.size" : {
          "title" : "Page Size",
          "type" : "object",
          "propertyOrder" : 3,
          "description" : "The number of results per page returned from the underlying datastore.
If the result set is smaller than the page size, the number of results will never be paginated.
If larger, the number of pages returned will be <code>result set size / page size</code>. Larger
values will result in fewer round trips to the datastore when retrieving large result sets. Leave as
<code>0</code> to not enable pagination, and return all results in a single page.",
          "properties" : {
            "value" : {
              "type" : "integer",
```

```
              "required" : false
            },
            "inherited" : {
              "type" : "boolean",
              "required" : true
            }
          }
        },
        "org.forgerock.services.cts.store.vlv.page.size" : {
          "title" : "VLV Page Size",
          "type" : "object",
          "propertyOrder" : 4,
          "description" : "The number of results per page returned from the underlying datastore when
using VLVs. Larger values will result in fewer round trips to the datastore when retrieving large
result sets.",
          "properties" : {
            "value" : {
              "type" : "integer",
              "required" : false
            },
            "inherited" : {
              "type" : "boolean",
              "required" : true
            }
          }
        }
      }
    },
    "amconfig.org.forgerock.services.cts.store.external.section" : {
      "title" : "External Store Configuration",
      "type" : "object",
      "propertyOrder" : 1,
      "properties" : {
        "org.forgerock.services.cts.store.ssl.enabled" : {
          "title" : "SSL/TLS Enabled",
          "type" : "object",
          "propertyOrder" : 0,
          "description" : "",
          "properties" : {
            "value" : {
              "type" : "boolean",
              "required" : false
            },
            "inherited" : {
              "type" : "boolean",
              "required" : true
            }
          }
        },
        "org.forgerock.services.cts.store.starttls.enabled" : {
          "title" : "Start TLS",
          "type" : "object",
          "propertyOrder" : 1,
          "description" : "Specifies whether to use StartTLS for the connection.",
          "properties" : {
            "value" : {
              "type" : "boolean",
              "required" : false
            },
```

```
            "inherited" : {
              "type" : "boolean",
              "required" : true
            }
          }
        },
        "org.forgerock.services.cts.store.directory.name" : {
          "title" : "Connection String(s)",
          "type" : "object",
          "propertyOrder" : 2,
          "description" : "An ordered list of connection strings for LDAP directories. Each connection
 string is composed as follows: <code>HOST:PORT[|SERVERID[|SITEID]]</code>, where server and site
 IDs are optional parameters that will prioritize that connection to use from the specified nodes.
 Multiple connection strings should be comma-separated, e.g. <code>host1:389,host2:50389|server1|
site1,host3:50389</code>.",
          "properties" : {
            "value" : {
              "type" : "string",
              "required" : false
            },
            "inherited" : {
              "type" : "boolean",
              "required" : true
            }
          }
        },
        "org.forgerock.services.cts.store.loginid" : {
          "title" : "Login Id",
          "type" : "object",
          "propertyOrder" : 3,
          "description" : "",
          "properties" : {
            "value" : {
              "type" : "string",
              "required" : false
            },
            "inherited" : {
              "type" : "boolean",
              "required" : true
            }
          }
        },
        "org.forgerock.services.cts.store.password" : {
          "title" : "Password",
          "type" : "object",
          "propertyOrder" : 4,
          "description" : "",
          "properties" : {
            "value" : {
              "type" : "string",
              "required" : false,
              "format" : "password"
            },
            "inherited" : {
              "type" : "boolean",
              "required" : true
            }
          }
        },
```

```
        "org.forgerock.services.cts.store.heartbeat" : {
          "title" : "Heartbeat",
          "type" : "object",
          "propertyOrder" : 5,
          "description" : "",
          "properties" : {
            "value" : {
              "type" : "integer",
              "required" : false
            },
            "inherited" : {
              "type" : "boolean",
              "required" : true
            }
          }
        },
        "org.forgerock.services.cts.store.affinity.enabled" : {
          "title" : "Affinity Enabled",
          "type" : "object",
          "propertyOrder" : 6,
          "description" : "Enables affinity based request load balancing when accessing the CTS
 servers. It is imperative that the connection string setting is set to the same value for all OpenAM
 servers in the deployment when this feature is enabled.",
          "properties" : {
            "value" : {
              "type" : "boolean",
              "required" : false
            },
            "inherited" : {
              "type" : "boolean",
              "required" : true
            }
          }
        }
      }
    }
  }
}
```

Dashboard

Realm Operations

Resource path: `/realm-config/services/dashboard`

Resource version: `1.0`

create

Usage:

```
am> create Dashboard --realm Realm --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "assignedDashboard" : {
      "title" : "Available Dashboard Apps",
      "description" : "List of application dashboard names available by default for realms with the
 Dashboard service configured.",
      "propertyOrder" : 700,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    }
  }
}
```

delete

Usage:

```
am> delete Dashboard --realm Realm
```

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action Dashboard --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action Dashboard --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action Dashboard --realm Realm --actionName nextdescendents
```

read

Usage:

```
am> read Dashboard --realm Realm
```

update

Usage:

```
am> update Dashboard --realm Realm --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "assignedDashboard" : {
      "title" : "Available Dashboard Apps",
      "description" : "List of application dashboard names available by default for realms with the
 Dashboard service configured.",
      "propertyOrder" : 700,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    }
  }
}
```

Global Operations

Resource path: `/global-config/services/dashboard`

Resource version: `1.0`

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action Dashboard --global --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action Dashboard --global --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action Dashboard --global --actionName nextdescendents
```

read

Usage:

```
am> read Dashboard --global
```

update

Usage:

```
am> update Dashboard --global --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "defaults" : {
      "properties" : {
        "assignedDashboard" : {
          "title" : "Available Dashboard Apps",
          "description" : "List of application dashboard names available by default for realms with
 the Dashboard service configured.",
          "propertyOrder" : 700,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        }
      },
      "type" : "object",
      "title" : "Realm Defaults"
    }
  }
}
```

DashboardInstance

Global Operations

Resource path: `/global-config/services/dashboard/instances`

Resource version: `1.0`

create

Usage:

```
am> create DashboardInstance --global --id id --body body
```

Parameters:

`--id`

The unique identifier for the resource.

`--body`

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
```

```
  "properties" : {
    "icfIdentifier" : {
      "title" : "ICF Identifier",
      "description" : "",
      "propertyOrder" : 600,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "name" : {
      "title" : "Dashboard Name",
      "description" : "The application name as it will appear to the administrator for configuring the
 dashboard.",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "login" : {
      "title" : "Dashboard Login",
      "description" : "The URL that takes the user to the application.",
      "propertyOrder" : 500,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "displayName" : {
      "title" : "Dashboard Display Name",
      "description" : "The application name that displays on the dashboard client.",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "className" : {
      "title" : "Dashboard Class Name",
      "description" : "Identifies how to access the application, for example
 <code>SAML2ApplicationClass</code> for a SAML v2.0 application.",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "icon" : {
      "title" : "Dashboard Icon",
      "description" : "The icon name that will be displayed on the dashboard client identifying the
 application.",
      "propertyOrder" : 400,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
```

delete

Usage:

```
am> delete DashboardInstance --global --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action DashboardInstance --global --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action DashboardInstance --global --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action DashboardInstance --global --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query DashboardInstance --global --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read DashboardInstance --global --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update DashboardInstance --global --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "icfIdentifier" : {
      "title" : "ICF Identifier",
      "description" : "",
      "propertyOrder" : 600,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "name" : {
      "title" : "Dashboard Name",
      "description" : "The application name as it will appear to the administrator for configuring the
 dashboard.",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "login" : {
      "title" : "Dashboard Login",
      "description" : "The URL that takes the user to the application.",
```

```
      "propertyOrder" : 500,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "displayName" : {
      "title" : "Dashboard Display Name",
      "description" : "The application name that displays on the dashboard client.",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "className" : {
      "title" : "Dashboard Class Name",
      "description" : "Identifies how to access the application, for example
 <code>SAML2ApplicationClass</code> for a SAML v2.0 application.",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "icon" : {
      "title" : "Dashboard Icon",
      "description" : "The icon name that will be displayed on the dashboard client identifying the
 application.",
      "propertyOrder" : 400,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
```

DashboardUserService

Realm Operations

Resource path: `/users/{user}/services/dashboard`

Resource version: `1.0`

create

Usage:

```
am> create DashboardUserService --realm Realm --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "assignedDashboard" : {
      "title" : "Assigned Dashboard",
      "description" : "",
      "propertyOrder" : 800,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    }
  }
}
```

delete

Usage:

```
am> delete DashboardUserService --realm Realm
```

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action DashboardUserService --realm Realm --user user --actionName getAllTypes
```

Parameters:

--user

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action DashboardUserService --realm Realm --user user --actionName getCreatableTypes
```

Parameters:

--user

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action DashboardUserService --realm Realm --user user --actionName nextdescendents
```

Parameters:

--user

read

Usage:

```
am> read DashboardUserService --realm Realm
```

unassignServices

action.unassignServices.description

Usage:

```
am> action DashboardUserService --realm Realm --body body --user user --actionName unassignServices
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "description" : "i18n:api-descriptor/UserServicesResource#schema.description",
  "type" : "object",
  "title" : "i18n:api-descriptor/UserServicesResource#schema.title",
  "properties" : {
    "serviceNames" : {
      "type" : "array",
      "title" : "i18n:api-descriptor/UserServicesResource#schema.servicename.title",
      "description" : "i18n:api-descriptor/UserServicesResource#schema.servicename.description",
      "items" : {
        "type" : "string"
      }
    }
  }
}
```

--user

update

Usage:

```
am> update DashboardUserService --realm Realm --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "assignedDashboard" : {
      "title" : "Assigned Dashboard",
      "description" : "",
      "propertyOrder" : 800,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    }
  }
}
```

Dashboards

Realm Operations

The dashboard service is responsible for returning information from the Dashboard. The only supported operation is read.

Resource path: `/dashboard`

Resource version: `1.0`

read

Read dashboard information

Usage:

```
am> read Dashboards --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

DataStoreDecision

Realm Operations

Resource path: `/realm-config/authentication/authenticationtrees/nodes/DataStoreDecisionNode`

Resource version: `1.0`

create

Usage:

```
am> create DataStoreDecision --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "required" : [ ]
}
```

delete

Usage:

```
am> delete DataStoreDecision --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action DataStoreDecision --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action DataStoreDecision --realm Realm --actionName getCreatableTypes
```

listOutcomes

List the available outcomes for the node type.

Usage:

```
am> action DataStoreDecision --realm Realm --body body --actionName listOutcomes
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "title" : "Some configuration of the node. This does not need to be complete against the
 configuration schema."
}
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action DataStoreDecision --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query DataStoreDecision --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read DataStoreDecision --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update DataStoreDecision --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "required" : [ ]
}
```

DataStoreInstance

Global Operations

Resource path: `/global-config/services/DataStoreService/config`

Resource version: `1.0`

create

Usage:

```
am> create DataStoreInstance --global --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "maximumConnectionPool" : {
      "title" : "Maximum Connection Pool Size",
      "description" : "",
      "propertyOrder" : 700,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "useSsl" : {
      "title" : "Use SSL",
      "description" : "",
      "propertyOrder" : 800,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "affinityEnabled" : {
      "title" : "Affinity Enabled",
      "description" : "",
      "propertyOrder" : 1000,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "minimumConnectionPool" : {
      "title" : "Minimum Connection Pool Size",
      "description" : "",
      "propertyOrder" : 600,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "useStartTLS" : {
      "title" : "Start TLS",
```

```
      "description" : "",
      "propertyOrder" : 900,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "bindPassword" : {
      "title" : "Bind Password",
      "description" : "",
      "propertyOrder" : 500,
      "required" : true,
      "type" : "string",
      "format" : "password",
      "exampleValue" : ""
    },
    "serverUrls" : {
      "title" : "Host Urls",
      "description" : "An ordered list of connection strings for LDAP directories.Each connection
 string is composed as follows: HOST:PORT. serverHostname = Host Name",
      "propertyOrder" : 200,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "bindDN" : {
      "title" : "Bind DN",
      "description" : "",
      "propertyOrder" : 400,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
```

delete

Usage:

```
am> delete DataStoreInstance --global --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action DataStoreInstance --global --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action DataStoreInstance --global --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action DataStoreInstance --global --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query DataStoreInstance --global --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read DataStoreInstance --global --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update DataStoreInstance --global --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "maximumConnectionPool" : {
      "title" : "Maximum Connection Pool Size",
      "description" : "",
      "propertyOrder" : 700,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "useSsl" : {
      "title" : "Use SSL",
      "description" : "",
      "propertyOrder" : 800,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "affinityEnabled" : {
      "title" : "Affinity Enabled",
      "description" : "",
      "propertyOrder" : 1000,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "minimumConnectionPool" : {
      "title" : "Minimum Connection Pool Size",
      "description" : "",
      "propertyOrder" : 600,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "useStartTLS" : {
      "title" : "Start TLS",
      "description" : "",
      "propertyOrder" : 900,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "bindPassword" : {
```

```
      "title" : "Bind Password",
      "description" : "",
      "propertyOrder" : 500,
      "required" : true,
      "type" : "string",
      "format" : "password",
      "exampleValue" : ""
    },
    "serverUrls" : {
      "title" : "Host Urls",
      "description" : "An ordered list of connection strings for LDAP directories.Each connection
 string is composed as follows: HOST:PORT. serverHostname = Host Name",
      "propertyOrder" : 200,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "bindDN" : {
      "title" : "Bind DN",
      "description" : "",
      "propertyOrder" : 400,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
```


DataStoreModule

Realm Operations

Resource path: `/realm-config/authentication/modules/datastore`

Resource version: `1.0`

create

Usage:

```
am> create DataStoreModule --realm Realm --id id --body body
```

Parameters:

`--id`

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "authenticationLevel" : {
      "title" : "Authentication Level",
      "description" : "The authentication level associated with this module.<br><br>Each
 authentication module has an authentication level that can be used to indicate the level of security
 associated with the module; 0 is the lowest (and the default).",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    }
  }
}
```

delete

Usage:

```
am> delete DataStoreModule --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action DataStoreModule --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action DataStoreModule --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action DataStoreModule --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query DataStoreModule --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read DataStoreModule --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update DataStoreModule --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "authenticationLevel" : {
      "title" : "Authentication Level",
      "description" : "The authentication level associated with this module.<br><br>Each
 authentication module has an authentication level that can be used to indicate the level of security
 associated with the module; 0 is the lowest (and the default).",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    }
  }
}
```

Global Operations

Resource path: `/global-config/authentication/modules/datastore`

Resource version: `1.0`

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action DataStoreModule --global --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action DataStoreModule --global --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action DataStoreModule --global --actionName nextdescendents
```

read

Usage:

```
am> read DataStoreModule --global
```

update

Usage:

```
am> update DataStoreModule --global --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "defaults" : {
      "properties" : {
        "authenticationLevel" : {
          "title" : "Authentication Level",
          "description" : "The authentication level associated with this module.<br><br>Each
 authentication module has an authentication level that can be used to indicate the level of security
 associated with the module; 0 is the lowest (and the default).",
          "propertyOrder" : 100,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        }
      },
      "type" : "object",
      "title" : "Realm Defaults"
    }
  }
}
```

DataStoreService

Realm Operations

Resource path: `/realm-config/services/DataStoreService`

Resource version: `1.0`

create

Usage:

```
am> create DataStoreService --realm Realm --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "policyDataStoreId" : {
      "title" : "Policy Data Store",
      "description" : "Select a data store configuration to be used for policy storage",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "applicationDataStoreId" : {
      "title" : "Application Data Store",
      "description" : "Select a data store configuration to be used for application storage",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
```

delete

Usage:

```
am> delete DataStoreService --realm Realm
```

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action DataStoreService --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action DataStoreService --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action DataStoreService --realm Realm --actionName nextdescendents
```

read

Usage:

```
am> read DataStoreService --realm Realm
```

update

Usage:

```
am> update DataStoreService --realm Realm --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "policyDataStoreId" : {
      "title" : "Policy Data Store",
      "description" : "Select a data store configuration to be used for policy storage",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "applicationDataStoreId" : {
      "title" : "Application Data Store",
      "description" : "Select a data store configuration to be used for application storage",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
```

Global Operations

Resource path: `/global-config/services/DataStoreService`

Resource version: `1.0`

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action DataStoreService --global --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action DataStoreService --global --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action DataStoreService --global --actionName nextdescendents
```

read

Usage:

```
am> read DataStoreService --global
```

update

Usage:

```
am> update DataStoreService --global --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "defaults" : {
      "properties" : {
        "applicationDataStoreId" : {
          "title" : "Application Data Store",
          "description" : "Select a data store configuration to be used for application storage",
          "propertyOrder" : 200,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "policyDataStoreId" : {
          "title" : "Policy Data Store",
          "description" : "Select a data store configuration to be used for policy storage",
          "propertyOrder" : 100,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      },
      "type" : "object",
      "title" : "Realm Defaults"
    }
  }
}
```

DecisionCombiners

Realm Operations

Service for querying and reading decision combiners information. Decision combiners describe how to resolve policy decisions when multiple policies apply

Resource path: `/decisioncombiners`

Resource version: `1.0`

query

Lists all decision combiners

Usage:

```
am> query DecisionCombiners --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all. Fields that can be queried: [title]

read

Reads an individual decision combiner specified by its name

Usage:

```
am> read DecisionCombiners --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

DefaultAdvancedProperties

Global Operations

An object of property key-value pairs

Resource path: `/global-config/servers/server-default/properties/advanced`

Resource version: `1.0`

read

Usage:

```
am> read DefaultAdvancedProperties --global
```

update

Usage:

```
am> update DefaultAdvancedProperties --global --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "patternProperties" : {
    ".+" : {
      "type" : "string",
      "title" : "Value",
      "description" : "Any string value"
    }
  },
  "$schema" : "http://json-schema.org/draft-04/schema#",
  "description" : "An object of property key-value pairs",
  "type" : "object",
  "title" : "Advanced Properties"
}
```

DefaultCtsDataStoreProperties

Global Operations

An object of property key-value pairs

Resource path: `/global-config/servers/server-default/properties/cts`

Resource version: `1.0`

read

Usage:

```
am> read DefaultCtsDataStoreProperties --global
```

update

Usage:

```
am> update DefaultCtsDataStoreProperties --global --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "amconfig.org.forgerock.services.cts.store.common.section" : {
      "title" : "CTS Token Store",
      "type" : "object",
      "propertyOrder" : 0,
```

```
      "properties" : {
        "org.forgerock.services.cts.store.location" : {
          "enum" : [ "default", "external" ],
          "options" : {
            "enum_titles" : [ "Default Token Store", "External Token Store" ]
          },
          "type" : "string",
          "title" : "Store Mode",
          "propertyOrder" : 0,
          "required" : true,
          "description" : ""
        },
        "org.forgerock.services.cts.store.root.suffix" : {
          "type" : "string",
          "title" : "Root Suffix",
          "propertyOrder" : 1,
          "required" : true,
          "description" : ""
        },
        "org.forgerock.services.cts.store.max.connections" : {
          "type" : "string",
          "title" : "Max Connections",
          "propertyOrder" : 2,
          "required" : true,
          "description" : ""
        },
        "org.forgerock.services.cts.store.page.size" : {
          "type" : "integer",
          "title" : "Page Size",
          "propertyOrder" : 3,
          "required" : true,
          "description" : "The number of results per page returned from the underlying datastore.
If the result set is smaller than the page size, the number of results will never be paginated.
If larger, the number of pages returned will be <code>result set size / page size</code>. Larger
values will result in fewer round trips to the datastore when retrieving large result sets. Leave as
<code>0</code> to not enable pagination, and return all results in a single page."
        },
        "org.forgerock.services.cts.store.vlv.page.size" : {
          "type" : "integer",
          "title" : "VLV Page Size",
          "propertyOrder" : 4,
          "required" : true,
          "description" : "The number of results per page returned from the underlying datastore when
using VLVs. Larger values will result in fewer round trips to the datastore when retrieving large
result sets."
        }
      }
    },
    "amconfig.org.forgerock.services.cts.store.external.section" : {
      "title" : "External Store Configuration",
      "type" : "object",
      "propertyOrder" : 1,
      "properties" : {
        "org.forgerock.services.cts.store.ssl.enabled" : {
          "type" : "boolean",
          "title" : "SSL/TLS Enabled",
          "propertyOrder" : 0,
          "required" : true,
          "description" : ""
```

```
        },
        "org.forgerock.services.cts.store.starttls.enabled" : {
          "type" : "boolean",
          "title" : "Start TLS",
          "propertyOrder" : 1,
          "required" : true,
          "description" : "Specifies whether to use StartTLS for the connection."
        },
        "org.forgerock.services.cts.store.directory.name" : {
          "type" : "string",
          "title" : "Connection String(s)",
          "propertyOrder" : 2,
          "required" : true,
          "description" : "An ordered list of connection strings for LDAP directories. Each connection
 string is composed as follows: <code>HOST:PORT[|SERVERID[|SITEID]]</code>, where server and site
 IDs are optional parameters that will prioritize that connection to use from the specified nodes.
 Multiple connection strings should be comma-separated, e.g. <code>host1:389,host2:50389|server1|
site1,host3:50389</code>."
        },
        "org.forgerock.services.cts.store.loginid" : {
          "type" : "string",
          "title" : "Login Id",
          "propertyOrder" : 3,
          "required" : true,
          "description" : ""
        },
        "org.forgerock.services.cts.store.password" : {
          "type" : "string",
          "title" : "Password",
          "propertyOrder" : 4,
          "required" : true,
          "description" : "",
          "format" : "password"
        },
        "org.forgerock.services.cts.store.heartbeat" : {
          "type" : "integer",
          "title" : "Heartbeat",
          "propertyOrder" : 5,
          "required" : true,
          "description" : ""
        },
        "org.forgerock.services.cts.store.affinity.enabled" : {
          "type" : "boolean",
          "title" : "Affinity Enabled",
          "propertyOrder" : 6,
          "required" : true,
          "description" : "Enables affinity based request load balancing when accessing the CTS
 servers. It is imperative that the connection string setting is set to the same value for all OpenAM
 servers in the deployment when this feature is enabled."
        }
      }
    }
  }
}
```

DefaultDirectoryConfiguration

Global Operations

Connection details for directory server(s).

Resource path: `/global-config/servers/server-default/properties/directoryConfiguration`

Resource version: `1.0`

read

Usage:

```
am> read DefaultDirectoryConfiguration --global
```

update

Usage:

```
am> update DefaultDirectoryConfiguration --global --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "directoryConfiguration" : {
      "type" : "object",
      "title" : "Directory Configuration",
      "propertyOrder" : 0,
      "properties" : {
        "minConnectionPool" : {
          "title" : "Minimum Connection Pool",
          "propertyOrder" : 0,
          "type" : "number"
        },
        "maxConnectionPool" : {
          "title" : "Maximum Connection Pool",
          "propertyOrder" : 1,
          "type" : "number"
        },
        "bindDn" : {
          "title" : "Bind DN",
          "propertyOrder" : 2,
          "type" : "string"
        },
        "bindPassword" : {
```

```
          "title" : "Bind Password",
          "propertyOrder" : 3,
          "type" : "string",
          "format" : "password"
        }
      }
    },
    "directoryServers" : {
      "type" : "array",
      "title" : "Server",
      "propertyOrder" : 1,
      "items" : {
        "type" : "object",
        "required" : [ "serverName", "hostName", "portNumber", "connectionType" ],
        "properties" : {
          "serverName" : {
            "title" : "Name",
            "type" : "string",
            "propertyOrder" : 0
          },
          "hostName" : {
            "title" : "Host Name",
            "type" : "string",
            "propertyOrder" : 1
          },
          "portNumber" : {
            "title" : "Port Number",
            "type" : "string",
            "propertyOrder" : 2
          },
          "connectionType" : {
            "type" : "string",
            "enum" : [ "SIMPLE", "SSL" ],
            "options" : {
              "enum_titles" : [ "SIMPLE", "SSL" ]
            },
            "title" : "Connection Type",
            "propertyOrder" : 3
          }
        }
      }
    }
  }
}
```

DefaultGeneralProperties

Global Operations

An object of property key-value pairs

Resource path: `/global-config/servers/server-default/properties/general`

Resource version: `1.0`

read

Usage:

```
am> read DefaultGeneralProperties --global
```

update

Usage:

```
am> update DefaultGeneralProperties --global --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "amconfig.header.installdir" : {
      "title" : "System",
      "type" : "object",
      "propertyOrder" : 0,
      "properties" : {
        "com.iplanet.services.configpath" : {
          "type" : "string",
          "title" : "Base installation directory",
          "propertyOrder" : 0,
          "required" : true,
          "description" : "Base directory where product's data resides. (property name:
 com.iplanet.services.configpath)"
        },
        "com.iplanet.am.locale" : {
          "type" : "string",
          "title" : "Default Locale",
          "propertyOrder" : 1,
          "required" : true,
          "description" : "Default locale for the product. (property name: com.iplanet.am.locale)"
        },
        "com.sun.identity.client.notification.url" : {
          "type" : "string",
          "title" : "Notification URL",
          "propertyOrder" : 2,
          "required" : true,
          "description" : "The location of notification service end point. It is usually the product's
 deployment URI/notificationservice. (property name: com.sun.identity.client.notification.url)"
        },
        "com.iplanet.am.util.xml.validating" : {
          "enum" : [ "on", "off" ],
          "options" : {
            "enum_titles" : [ "On", "Off" ]
          },
          "type" : "string",
          "title" : "XML Validation",
```

```
          "propertyOrder" : 3,
          "required" : true,
          "description" : "Specifies if validation is required when parsing XML documents. (property
name: com.iplanet.am.util.xml.validating)"
        }
      }
    },
    "amconfig.header.debug" : {
      "title" : "Debugging",
      "type" : "object",
      "propertyOrder" : 1,
      "properties" : {
        "com.iplanet.services.debug.level" : {
          "enum" : [ "off", "error", "warning", "message" ],
          "options" : {
            "enum_titles" : [ "Off", "Error", "Warning", "Message" ]
          },
          "type" : "string",
          "title" : "Debug Level",
          "propertyOrder" : 0,
          "required" : true,
          "description" : "Debug level for all components in the product. (property name:
com.iplanet.services.debug.level)"
        },
        "com.sun.services.debug.mergeall" : {
          "enum" : [ "on", "off" ],
          "options" : {
            "enum_titles" : [ "On", "Off" ]
          },
          "type" : "string",
          "title" : "Merge Debug Files",
          "propertyOrder" : 1,
          "required" : true,
          "description" : "On : Directs all debug data to a single file (debug.out); Off : creates
separate per-component debug files (property name : com.sun.services.debug.mergeall)"
        },
        "com.iplanet.services.debug.directory" : {
          "type" : "string",
          "title" : "Debug Directory",
          "propertyOrder" : 2,
          "required" : true,
          "description" : "Directory where debug files reside. (property name:
com.iplanet.services.debug.directory)"
        }
      }
    },
    "amconfig.header.mailserver" : {
      "title" : "Mail Server",
      "type" : "object",
      "propertyOrder" : 2,
      "properties" : {
        "com.iplanet.am.smtphost" : {
          "type" : "string",
          "title" : "Mail Server Host Name",
          "propertyOrder" : 0,
          "required" : true,
          "description" : "(property name: com.iplanet.am.smtphost)"
        },
        "com.iplanet.am.smtpport" : {
```

```
          "type" : "integer",
          "title" : "Mail Server Port Number",
          "propertyOrder" : 1,
          "required" : true,
          "description" : "(property name: com.iplanet.am.smtpport)"
        }
      }
    }
  }
}
```

DefaultSdkProperties

Global Operations

An object of property key-value pairs

Resource path: `/global-config/servers/server-default/properties/sdk`

Resource version: `1.0`

read

Usage:

```
am> read DefaultSdkProperties --global
```

update

Usage:

```
am> update DefaultSdkProperties --global --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "amconfig.header.datastore" : {
      "title" : "Data Store",
      "type" : "object",
      "propertyOrder" : 0,
      "properties" : {
        "com.sun.identity.sm.enableDataStoreNotification" : {
          "type" : "boolean",
          "title" : "Enable Datastore Notification",
```

```
          "propertyOrder" : 0,
          "required" : true,
          "description" : "Specifies if backend datastore notification is enabled. If
this value is set to 'false', then in-memory notification is enabled. (property name:
com.sun.identity.sm.enableDataStoreNotification)"
        },
        "com.sun.identity.sm.notification.threadpool.size" : {
          "type" : "integer",
          "title" : "Notification Pool Size",
          "propertyOrder" : 1,
          "required" : true,
          "description" : "Specifies the size of the sm notification thread pool (total number of
threads). (property name: com.sun.identity.sm.notification.threadpool.size)"
        }
      }
    },
    "amconfig.header.eventservice" : {
      "title" : "Event Service",
      "type" : "object",
      "propertyOrder" : 1,
      "properties" : {
        "com.iplanet.am.event.connection.num.retries" : {
          "type" : "integer",
          "title" : "Number of retries for Event Service connections",
          "propertyOrder" : 0,
          "required" : true,
          "description" : "Specifies the number of attempts made to successfully re-establish the
Event Service connections. (property name: com.iplanet.am.event.connection.num.retries)"
        },
        "com.iplanet.am.event.connection.delay.between.retries" : {
          "type" : "integer",
          "title" : "Delay between Event Service connection retries",
          "propertyOrder" : 1,
          "required" : true,
          "description" : "Specifies the delay in milliseconds between retries to re-establish the
Event Service connections. (property name: com.iplanet.am.event.connection.delay.between.retries)"
        },
        "com.iplanet.am.event.connection.ldap.error.codes.retries" : {
          "type" : "string",
          "title" : "Error codes for Event Service connection retries",
          "propertyOrder" : 2,
          "required" : true,
          "description" : "This secifies the LDAP exception error codes for which
retries to re-establish Event Service connections will trigger. (property name:
com.iplanet.am.event.connection.ldap.error.codes.retries)"
        },
        "com.sun.am.event.connection.disable.list" : {
          "type" : "string",
          "title" : "Disabled Event Service Connection",
          "propertyOrder" : 3,
          "required" : true,
          "description" : "Specifies which event connection (persistent search) to be disabled. There
are three valid values - aci, sm and um (case insensitive). Multiple values should be separated with
\",\". (property name: com.sun.am.event.connection.disable.list)"
        }
      }
    },
    "amconfig.header.ldapconnection" : {
      "title" : "LDAP Connection",
```

```
     "type" : "object",
     "propertyOrder" : 2,
     "properties" : {
       "com.iplanet.am.ldap.connection.num.retries" : {
         "type" : "integer",
         "title" : "Number of retries for LDAP Connection",
         "propertyOrder" : 0,
         "required" : true,
         "description" : "Specifies the number of attempts made to successfully re-establish LDAP
Connection. (property name: com.iplanet.am.ldap.connection.num.retries)"
       },
       "com.iplanet.am.ldap.connection.delay.between.retries" : {
         "type" : "integer",
         "title" : "Delay between LDAP connection retries",
         "propertyOrder" : 1,
         "required" : true,
         "description" : "Specifies the delay in milliseconds between retries to re-establish the
LDAP connections. (property name: com.iplanet.am.ldap.connection.delay.between.retries)"
       },
       "com.iplanet.am.ldap.connection.ldap.error.codes.retries" : {
         "type" : "string",
         "title" : "Error codes for LDAP connection retries",
         "propertyOrder" : 2,
         "required" : true,
         "description" : "This secifies the LDAP exception error codes for
which retries to re-establish LDAP connections will trigger. (property name:
com.iplanet.am.ldap.connection.ldap.error.codes.retries)"
       }
     }
   },
   "amconfig.header.cachingreplica" : {
     "title" : "Caching and Replica",
     "type" : "object",
     "propertyOrder" : 3,
     "properties" : {
       "com.iplanet.am.sdk.cache.maxSize" : {
         "type" : "integer",
         "title" : "SDK Caching Max. Size",
         "propertyOrder" : 0,
         "required" : true,
         "description" : "Specifies the size of the cache when SDK caching is enabled. The size
should be an integer greater than 0, or default size (10000) will be used. Changing this value will
reset (clear) the contents of the cache. (property name: com.iplanet.am.sdk.cache.maxSize)"
       }
     }
   },
   "amconfig.header.sdktimetoliveconfig" : {
     "title" : "Time To Live Configuration",
     "type" : "object",
     "propertyOrder" : 4,
     "properties" : {
       "com.iplanet.am.sdk.cache.entry.expire.enabled" : {
         "type" : "boolean",
         "title" : "Cache Entry Expiration Enabled",
         "propertyOrder" : 0,
         "required" : true,
         "description" : "If this property is set, the cache entries will expire
based on the time specified in User Entry Expiration Time property. (property name:
com.iplanet.am.sdk.cache.entry.expire.enabled)"
```

```
        },
        "com.iplanet.am.sdk.cache.entry.user.expire.time" : {
          "type" : "integer",
          "title" : "User Entry Expiration Time",
          "propertyOrder" : 1,
          "required" : true,
          "description" : "This property specifies time in minutes for which the user entries remain
 valid in cache after their last modification. After this specified period of time elapses (after the
 last modification/read from the directory), the data for the entry that is cached will expire. At
 that instant new requests for data for these user entries will result in reading from the Directory.
 (property name: com.iplanet.am.sdk.cache.entry.user.expire.time)"
        },
        "com.iplanet.am.sdk.cache.entry.default.expire.time" : {
          "type" : "integer",
          "title" : "Default Entry Expiration Time",
          "propertyOrder" : 2,
          "required" : true,
          "description" : "This property specifies time in minutes for which the non-user entries
 remain valid in cache after their last modification. After this specified period of time elapses
 (after the last modification/read from the directory), the data for the entry that is cached will
 expire. At that instant new requests for data for these non-user entries will result in reading from
 the Directory. (property name: com.iplanet.am.sdk.cache.entry.default.expire.time)"
        }
      }
    }
  }
}
```

DefaultSecurityProperties

Global Operations

An object of property key-value pairs

Resource path: `/global-config/servers/server-default/properties/security`

Resource version: `1.0`

read

Usage:

```
am> read DefaultSecurityProperties --global
```

update

Usage:

```
am> update DefaultSecurityProperties --global --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "amconfig.header.encryption" : {
      "title" : "Encryption",
      "type" : "object",
      "propertyOrder" : 0,
      "properties" : {
        "am.encryption.pwd" : {
          "type" : "string",
          "title" : "Password Encryption Key",
          "propertyOrder" : 0,
          "required" : true,
          "description" : "The encryption key value for decrypting passwords stored in the Service
 Management System configuration. (property name: am.encryption.pwd)"
        },
        "com.iplanet.security.encryptor" : {
          "type" : "string",
          "title" : "Encryption class",
          "propertyOrder" : 1,
          "required" : true,
          "description" : "The default encryption class. (property name:
 com.iplanet.security.encryptor)"
        },
        "com.iplanet.security.SecureRandomFactoryImpl" : {
          "type" : "string",
          "title" : "Secure Random Factory Class",
          "propertyOrder" : 2,
          "required" : true,
          "description" : "This property is used for specifying SecureRandomFactory class. Available
 values for this property are com.iplanet.am.util.JSSSecureRandomFactoryImpl that is using JSS
 and com.iplanet.am.util.SecureRandomFactoryImpl that is using pure Java only. (property name:
 com.iplanet.security.SecureRandomFactoryImpl)"
        }
      }
    },
    "amconfig.header.validation" : {
      "title" : "Validation",
      "type" : "object",
      "propertyOrder" : 1,
      "properties" : {
        "com.iplanet.services.comm.server.pllrequest.maxContentLength" : {
          "type" : "integer",
          "title" : "Platform Low Level Comm. Max. Content Length",
          "propertyOrder" : 0,
          "required" : true,
          "description" : "Maximum content-length for an HttpRequest. (property name:
 com.iplanet.services.comm.server.pllrequest.maxContentLength)"
        },
        "com.iplanet.am.clientIPCheckEnabled" : {
          "type" : "boolean",
          "title" : "Client IP Address Check",
          "propertyOrder" : 1,
```

```
          "required" : true,
          "description" : "Specifies whether or not the IP address of the client is checked in all
single sign on token creations or validations. (property name: com.iplanet.am.clientIPCheckEnabled)"
        }
      }
    },
    "amconfig.header.cookie" : {
      "title" : "Cookie",
      "type" : "object",
      "propertyOrder" : 2,
      "properties" : {
        "com.iplanet.am.cookie.name" : {
          "type" : "string",
          "title" : "Cookie Name",
          "propertyOrder" : 0,
          "required" : true,
          "description" : "The cookie name used by Authentication Service to set the valid
session handler ID. This name is used to retrieve the valid session information. (property name:
com.iplanet.am.cookie.name)"
        },
        "com.iplanet.am.cookie.secure" : {
          "type" : "boolean",
          "title" : "Secure Cookie",
          "propertyOrder" : 1,
          "required" : true,
          "description" : "Specifies whether to set cookie in a secure mode in which the browser
will only return the cookie when a secure protocol such as HTTP(s) is used. (property name:
com.iplanet.am.cookie.secure)"
        },
        "com.iplanet.am.cookie.encode" : {
          "type" : "boolean",
          "title" : "Encode Cookie Value",
          "propertyOrder" : 2,
          "required" : true,
          "description" : "Specifies whether to URL encode the cookie value. (property name:
com.iplanet.am.cookie.encode)"
        }
      }
    },
    "amconfig.header.securitykey" : {
      "title" : "Key Store",
      "type" : "object",
      "propertyOrder" : 3,
      "properties" : {
        "com.sun.identity.saml.xmlsig.keystore" : {
          "type" : "string",
          "title" : "Keystore File",
          "propertyOrder" : 0,
          "required" : true,
          "description" : "Specifies the location of the keystore file. (property name:
com.sun.identity.saml.xmlsig.keystore)"
        },
        "com.sun.identity.saml.xmlsig.storetype" : {
          "type" : "string",
          "title" : "Keystore Type",
          "propertyOrder" : 1,
          "required" : true,
          "description" : "Specifies the keystore type. (property name:
com.sun.identity.saml.xmlsig.storetype)"
```

```
        },
        "com.sun.identity.saml.xmlsig.storepass" : {
          "type" : "string",
          "title" : "Keystore Password File",
          "propertyOrder" : 2,
          "required" : true,
          "description" : "Specifies the location of the file that contains the password used to
access the keystore file. (property name: com.sun.identity.saml.xmlsig.storepass)"
        },
        "com.sun.identity.saml.xmlsig.keypass" : {
          "type" : "string",
          "title" : "Private Key Password File",
          "propertyOrder" : 3,
          "required" : true,
          "description" : "Specifies the location of the file that contains the
password used to protect the private key of a generated key pair. (property name:
com.sun.identity.saml.xmlsig.keypass)"
        },
        "com.sun.identity.saml.xmlsig.certalias" : {
          "type" : "string",
          "title" : "Certificate Alias",
          "propertyOrder" : 4,
          "required" : true,
          "description" : "(property name: com.sun.identity.saml.xmlsig.certalias)"
        }
      }
    },
    "amconfig.header.crlcache" : {
      "title" : "Certificate Revocation List Caching",
      "type" : "object",
      "propertyOrder" : 4,
      "properties" : {
        "com.sun.identity.crl.cache.directory.host" : {
          "type" : "string",
          "title" : "LDAP server host name",
          "propertyOrder" : 0,
          "required" : true,
          "description" : ""
        },
        "com.sun.identity.crl.cache.directory.port" : {
          "type" : "integer",
          "title" : "LDAP server port number",
          "propertyOrder" : 1,
          "required" : true,
          "description" : ""
        },
        "com.sun.identity.crl.cache.directory.ssl" : {
          "type" : "boolean",
          "title" : "SSL/TLS Enabled",
          "propertyOrder" : 2,
          "required" : true,
          "description" : ""
        },
        "com.sun.identity.crl.cache.directory.user" : {
          "type" : "string",
          "title" : "LDAP server bind user name",
          "propertyOrder" : 3,
          "required" : true,
          "description" : ""
```

```
        },
        "com.sun.identity.crl.cache.directory.password" : {
          "type" : "string",
          "title" : "LDAP server bind password",
          "propertyOrder" : 4,
          "required" : true,
          "description" : "",
          "format" : "password"
        },
        "com.sun.identity.crl.cache.directory.searchlocs" : {
          "type" : "string",
          "title" : "LDAP search base DN",
          "propertyOrder" : 5,
          "required" : true,
          "description" : ""
        },
        "com.sun.identity.crl.cache.directory.searchattr" : {
          "type" : "string",
          "title" : "Search Attributes",
          "propertyOrder" : 6,
          "required" : true,
          "description" : "Any DN component of issuer's subjectDN can be used to retrieve CRL from
local LDAP server. It is single value string, like, \"cn\". All Root CA need to use the same search
attribute."
        }
      }
    },
    "amconfig.header.ocsp.check" : {
      "title" : "Online Certificate Status Protocol Check",
      "type" : "object",
      "propertyOrder" : 5,
      "properties" : {
        "com.sun.identity.authentication.ocspCheck" : {
          "type" : "boolean",
          "title" : "Check Enabled",
          "propertyOrder" : 0,
          "required" : true,
          "description" : ""
        },
        "com.sun.identity.authentication.ocsp.responder.url" : {
          "type" : "string",
          "title" : "Responder URL",
          "propertyOrder" : 1,
          "required" : true,
          "description" : ""
        },
        "com.sun.identity.authentication.ocsp.responder.nickname" : {
          "type" : "string",
          "title" : "Certificate Nickname",
          "propertyOrder" : 2,
          "required" : true,
          "description" : ""
        }
      }
    },
    "amconfig.header.deserialisationwhitelist" : {
      "title" : "Object Deserialisation Class Whitelist",
      "type" : "object",
      "propertyOrder" : 6,
```

```
      "properties" : {
        "openam.deserialisation.classes.whitelist" : {
          "type" : "string",
          "title" : "Whitelist",
          "propertyOrder" : 0,
          "required" : true,
          "description" : "The list of classes that are considered valid when OpenAM performs
 Object deserialisation operations. The defaults should work for most installations. (property name:
 openam.deserialisation.classes.whitelist)"
        }
      }
    }
  }
}
```

DefaultSessionProperties

Global Operations

An object of property key-value pairs

Resource path: `/global-config/servers/server-default/properties/session`

Resource version: `1.0`

read

Usage:

```
am> read DefaultSessionProperties --global
```

update

Usage:

```
am> update DefaultSessionProperties --global --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "amconfig.header.sessionthresholds" : {
      "title" : "Session Limits",
      "type" : "object",
      "propertyOrder" : 0,
```

```
     "properties" : {
       "org.forgerock.openam.session.service.access.persistence.caching.maxsize" : {
         "type" : "integer",
         "title" : "Maximum Session Cache Size",
         "propertyOrder" : 0,
         "required" : true,
         "description" : "The maximum number of sessions to cache in the per-server internal session
cache. (property name: org.forgerock.openam.session.service.access.persistence.caching.maxsize)"
       },
       "com.iplanet.am.session.invalidsessionmaxtime" : {
         "type" : "integer",
         "title" : "Invalidate Session Max Time",
         "propertyOrder" : 1,
         "required" : true,
         "description" : "Duration in minutes after which the invalid session will be removed
from the session table if it is created and the user does not login. This value should always
be greater than the timeout value in the Authentication module properties file. (property name:
com.iplanet.am.session.invalidsessionmaxtime)"
       }
     }
   },
   "amconfig.header.sessionlogging" : {
     "title" : "Statistics",
     "type" : "object",
     "propertyOrder" : 1,
     "properties" : {
       "com.iplanet.am.stats.interval" : {
         "type" : "integer",
         "title" : "Logging Interval (in seconds)",
         "propertyOrder" : 0,
         "required" : true,
         "description" : "Number of seconds to elapse between statistics logging. The interval
should be at least 5 seconds to avoid CPU saturation. An interval value less than 5 seconds will be
interpreted as 5 seconds. (property name: com.iplanet.am.stats.interval)"
       },
       "com.iplanet.services.stats.state" : {
         "enum" : [ "off", "file", "console" ],
         "options" : {
           "enum_titles" : [ "Off", "File", "Console" ]
         },
         "type" : "string",
         "title" : "State",
         "propertyOrder" : 1,
         "required" : true,
         "description" : "Statistics state 'file' will write to a file under the specified directory,
and 'console' will write into webserver log files. (property name: com.iplanet.services.stats.state)"
       },
       "com.iplanet.services.stats.directory" : {
         "type" : "string",
         "title" : "Directory",
         "propertyOrder" : 2,
         "required" : true,
         "description" : "Directory where the statistic files will be created. Use forward slashes
\"/\" to separate directories, not backslash \"\\\". Spaces in the file name are allowed for Windows.
(property name: com.iplanet.services.stats.directory)"
       },
       "com.sun.am.session.enableHostLookUp" : {
         "type" : "boolean",
         "title" : "Enable Host Lookup",
```

```
          "propertyOrder" : 3,
          "required" : true,
          "description" : "Enables or disables host lookup during session logging. (property name:
 com.sun.am.session.enableHostLookUp)"
        }
      }
    },
    "amconfig.header.sessionnotification" : {
      "title" : "Notification",
      "type" : "object",
      "propertyOrder" : 2,
      "properties" : {
        "com.iplanet.am.notification.threadpool.size" : {
          "type" : "integer",
          "title" : "Notification Pool Size",
          "propertyOrder" : 0,
          "required" : true,
          "description" : "Specifies the size of the notification thread pool (total number of
 threads). (property name: com.iplanet.am.notification.threadpool.size)"
        },
        "com.iplanet.am.notification.threadpool.threshold" : {
          "type" : "integer",
          "title" : "Notification Thread Pool Threshold",
          "propertyOrder" : 1,
          "required" : true,
          "description" : "Specifies the maximum task queue length for serving notification threads.
 (property name: com.iplanet.am.notification.threadpool.threshold)"
        }
      }
    },
    "amconfig.header.sessionvalidation" : {
      "title" : "Validation",
      "type" : "object",
      "propertyOrder" : 3,
      "properties" : {
        "com.sun.am.session.caseInsensitiveDN" : {
          "type" : "boolean",
          "title" : "Case Insensitive client DN comparison",
          "propertyOrder" : 0,
          "required" : true,
          "description" : "Specifies if client distinguished name comparison is case insensitive/
sensitive. (property name: com.sun.am.session.caseInsensitiveDN)"
        }
      }
    }
  }
}
```

DefaultUmaDataStoreProperties

Global Operations

An object of property key-value pairs

Resource path: `/global-config/servers/server-default/properties/uma`

Resource version: `1.0`

read

Usage:

```
am> read DefaultUmaDataStoreProperties --global
```

update

Usage:

```
am> update DefaultUmaDataStoreProperties --global --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "amconfig.org.forgerock.services.resourcesets.store.common.section" : {
      "title" : "UMA Resource Store",
      "type" : "object",
      "propertyOrder" : 0,
      "properties" : {
        "org.forgerock.services.resourcesets.store.location" : {
          "enum" : [ "default", "external" ],
          "options" : {
            "enum_titles" : [ "Default Token Store", "External Token Store" ]
          },
          "type" : "string",
          "title" : "Store Mode",
          "propertyOrder" : 0,
          "required" : true,
          "description" : ""
        },
        "org.forgerock.services.resourcesets.store.root.suffix" : {
          "type" : "string",
          "title" : "Root Suffix",
          "propertyOrder" : 1,
          "required" : true,
          "description" : ""
        },
        "org.forgerock.services.resourcesets.store.max.connections" : {
          "type" : "string",
          "title" : "Max Connections",
          "propertyOrder" : 2,
          "required" : true,
          "description" : ""
```

```
        }
      }
    },
    "amconfig.org.forgerock.services.resourcesets.store.external.section" : {
      "title" : "External UMA Resource Store Configuration",
      "type" : "object",
      "propertyOrder" : 1,
      "properties" : {
        "org.forgerock.services.resourcesets.store.ssl.enabled" : {
          "type" : "boolean",
          "title" : "SSL/TLS Enabled",
          "propertyOrder" : 0,
          "required" : true,
          "description" : ""
        },
        "org.forgerock.services.resourcesets.store.starttls.enabled" : {
          "type" : "boolean",
          "title" : "Start TLS",
          "propertyOrder" : 1,
          "required" : true,
          "description" : "Specifies whether to use StartTLS for the connection."
        },
        "org.forgerock.services.resourcesets.store.directory.name" : {
          "type" : "string",
          "title" : "Connection String(s)",
          "propertyOrder" : 2,
          "required" : true,
          "description" : "An ordered list of connection strings for LDAP directories. Each connection
 string is composed as follows: <code>HOST:PORT[|SERVERID[|SITEID]]</code>, where server and site
 IDs are optional parameters that will prioritize that connection to use from the specified nodes.
 Multiple connection strings should be comma-separated, e.g. <code>host1:389,host2:50389|server1|
site1,host3:50389</code>."
        },
        "org.forgerock.services.resourcesets.store.loginid" : {
          "type" : "string",
          "title" : "Login Id",
          "propertyOrder" : 3,
          "required" : true,
          "description" : ""
        },
        "org.forgerock.services.resourcesets.store.password" : {
          "type" : "string",
          "title" : "Password",
          "propertyOrder" : 4,
          "required" : true,
          "description" : "",
          "format" : "password"
        },
        "org.forgerock.services.resourcesets.store.heartbeat" : {
          "type" : "integer",
          "title" : "Heartbeat",
          "propertyOrder" : 5,
          "required" : true,
          "description" : ""
        }
      }
    },
    "amconfig.org.forgerock.services.umaaudit.store.common.section" : {
      "title" : "UMA Audit Store",
```

```
      "type" : "object",
      "propertyOrder" : 2,
      "properties" : {
        "org.forgerock.services.umaaudit.store.location" : {
          "enum" : [ "default", "external" ],
          "options" : {
            "enum_titles" : [ "Default Token Store", "External Token Store" ]
          },
          "type" : "string",
          "title" : "Store Mode",
          "propertyOrder" : 0,
          "required" : true,
          "description" : ""
        },
        "org.forgerock.services.umaaudit.store.root.suffix" : {
          "type" : "string",
          "title" : "Root Suffix",
          "propertyOrder" : 1,
          "required" : true,
          "description" : ""
        },
        "org.forgerock.services.umaaudit.store.max.connections" : {
          "type" : "string",
          "title" : "Max Connections",
          "propertyOrder" : 2,
          "required" : true,
          "description" : ""
        }
      }
    },
    "amconfig.org.forgerock.services.umaaudit.store.external.section" : {
      "title" : "External UMA Audit Store Configuration",
      "type" : "object",
      "propertyOrder" : 3,
      "properties" : {
        "org.forgerock.services.umaaudit.store.ssl.enabled" : {
          "type" : "boolean",
          "title" : "SSL/TLS Enabled",
          "propertyOrder" : 0,
          "required" : true,
          "description" : ""
        },
        "org.forgerock.services.umaaudit.store.starttls.enabled" : {
          "type" : "boolean",
          "title" : "Start TLS",
          "propertyOrder" : 1,
          "required" : true,
          "description" : "Specifies whether to use StartTLS for the connection."
        },
        "org.forgerock.services.umaaudit.store.directory.name" : {
          "type" : "string",
          "title" : "Connection String(s)",
          "propertyOrder" : 2,
          "required" : true,
          "description" : "An ordered list of connection strings for LDAP directories. Each connection
 string is composed as follows: <code>HOST:PORT[|SERVERID[|SITEID]]</code>, where server and site
 IDs are optional parameters that will prioritize that connection to use from the specified nodes.
 Multiple connection strings should be comma-separated, e.g. <code>host1:389,host2:50389|server1|
site1,host3:50389</code>."
```

```
      },
      "org.forgerock.services.umaaudit.store.loginid" : {
        "type" : "string",
        "title" : "Login Id",
        "propertyOrder" : 3,
        "required" : true,
        "description" : ""
      },
      "org.forgerock.services.umaaudit.store.password" : {
        "type" : "string",
        "title" : "Password",
        "propertyOrder" : 4,
        "required" : true,
        "description" : "",
        "format" : "password"
      },
      "org.forgerock.services.umaaudit.store.heartbeat" : {
        "type" : "integer",
        "title" : "Heartbeat",
        "propertyOrder" : 5,
        "required" : true,
        "description" : ""
      }
    }
  },
  "amconfig.org.forgerock.services.uma.pendingrequests.store.common.section" : {
    "title" : "Pending Requests Store",
    "type" : "object",
    "propertyOrder" : 4,
    "properties" : {
      "org.forgerock.services.uma.pendingrequests.store.location" : {
        "enum" : [ "default", "external" ],
        "options" : {
          "enum_titles" : [ "Default Token Store", "External Token Store" ]
        },
        "type" : "string",
        "title" : "Store Mode",
        "propertyOrder" : 0,
        "required" : true,
        "description" : ""
      },
      "org.forgerock.services.uma.pendingrequests.store.root.suffix" : {
        "type" : "string",
        "title" : "Root Suffix",
        "propertyOrder" : 1,
        "required" : true,
        "description" : ""
      },
      "org.forgerock.services.uma.pendingrequests.store.max.connections" : {
        "type" : "string",
        "title" : "Max Connections",
        "propertyOrder" : 2,
        "required" : true,
        "description" : ""
      }
    }
  },
  "amconfig.org.forgerock.services.uma.pendingrequests.store.external.section" : {
    "title" : "External Pending Requests Store Configuration",
```

```
      "type" : "object",
      "propertyOrder" : 5,
      "properties" : {
        "org.forgerock.services.uma.pendingrequests.store.ssl.enabled" : {
          "type" : "boolean",
          "title" : "SSL/TLS Enabled",
          "propertyOrder" : 0,
          "required" : true,
          "description" : ""
        },
        "org.forgerock.services.uma.pendingrequests.store.starttls.enabled" : {
          "type" : "boolean",
          "title" : "Start TLS",
          "propertyOrder" : 1,
          "required" : true,
          "description" : "Specifies whether to use StartTLS for the connection."
        },
        "org.forgerock.services.uma.pendingrequests.store.directory.name" : {
          "type" : "string",
          "title" : "Connection String(s)",
          "propertyOrder" : 2,
          "required" : true,
          "description" : "An ordered list of connection strings for LDAP directories. Each connection
 string is composed as follows: <code>HOST:PORT[|SERVERID[|SITEID]]</code>, where server and site
 IDs are optional parameters that will prioritize that connection to use from the specified nodes.
 Multiple connection strings should be comma-separated, e.g. <code>host1:389,host2:50389|server1|
site1,host3:50389</code>."
        },
        "org.forgerock.services.uma.pendingrequests.store.loginid" : {
          "type" : "string",
          "title" : "Login Id",
          "propertyOrder" : 3,
          "required" : true,
          "description" : ""
        },
        "org.forgerock.services.uma.pendingrequests.store.password" : {
          "type" : "string",
          "title" : "Password",
          "propertyOrder" : 4,
          "required" : true,
          "description" : "",
          "format" : "password"
        },
        "org.forgerock.services.uma.pendingrequests.store.heartbeat" : {
          "type" : "integer",
          "title" : "Heartbeat",
          "propertyOrder" : 5,
          "required" : true,
          "description" : ""
        }
      }
    },
    "amconfig.org.forgerock.services.uma.labels.store.common.section" : {
      "title" : "UMA Resource Labels Store",
      "type" : "object",
      "propertyOrder" : 6,
      "properties" : {
        "org.forgerock.services.uma.labels.store.location" : {
          "enum" : [ "default", "external" ],
```

```
          "options" : {
            "enum_titles" : [ "Default Token Store", "External Token Store" ]
          },
          "type" : "string",
          "title" : "Store Mode",
          "propertyOrder" : 0,
          "required" : true,
          "description" : ""
        },
        "org.forgerock.services.uma.labels.store.root.suffix" : {
          "type" : "string",
          "title" : "Root Suffix",
          "propertyOrder" : 1,
          "required" : true,
          "description" : ""
        },
        "org.forgerock.services.uma.labels.store.max.connections" : {
          "type" : "string",
          "title" : "Max Connections",
          "propertyOrder" : 2,
          "required" : true,
          "description" : ""
        }
      }
    },
    "amconfig.org.forgerock.services.uma.labels.store.external.section" : {
      "title" : "External UMA Resource Labels Store Configuration",
      "type" : "object",
      "propertyOrder" : 7,
      "properties" : {
        "org.forgerock.services.uma.labels.store.ssl.enabled" : {
          "type" : "boolean",
          "title" : "SSL/TLS Enabled",
          "propertyOrder" : 0,
          "required" : true,
          "description" : ""
        },
        "org.forgerock.services.uma.labels.store.starttls.enabled" : {
          "type" : "boolean",
          "title" : "Start TLS",
          "propertyOrder" : 1,
          "required" : true,
          "description" : "Specifies whether to use StartTLS for the connection."
        },
        "org.forgerock.services.uma.labels.store.directory.name" : {
          "type" : "string",
          "title" : "Connection String(s)",
          "propertyOrder" : 2,
          "required" : true,
          "description" : "An ordered list of connection strings for LDAP directories. Each connection
 string is composed as follows: <code>HOST:PORT[|SERVERID[|SITEID]]</code>, where server and site
 IDs are optional parameters that will prioritize that connection to use from the specified nodes.
 Multiple connection strings should be comma-separated, e.g. <code>host1:389,host2:50389|server1|
site1,host3:50389</code>."
        },
        "org.forgerock.services.uma.labels.store.loginid" : {
          "type" : "string",
          "title" : "Login Id",
          "propertyOrder" : 3,
```

```
          "required" : true,
          "description" : ""
        },
        "org.forgerock.services.uma.labels.store.password" : {
          "type" : "string",
          "title" : "Password",
          "propertyOrder" : 4,
          "required" : true,
          "description" : "",
          "format" : "password"
        },
        "org.forgerock.services.uma.labels.store.heartbeat" : {
          "type" : "integer",
          "title" : "Heartbeat",
          "propertyOrder" : 5,
          "required" : true,
          "description" : ""
        }
      }
    }
  }
}
```

DeviceGeofencing

Realm Operations

Resource path: `/realm-config/authentication/authenticationtrees/nodes/DeviceGeoFencingNode`

Resource version: `1.0`

create

Usage:

```
am> create DeviceGeofencing --realm Realm --id id --body body
```

Parameters:

`--id`

The unique identifier for the resource.

`--body`

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "locations" : {
      "title" : "Trusted Locations",
      "description" : "Specify the latitude and longitude of trusted locations. Separate the values
 with a comma; for example, `-123.177201,49.164532`.",
      "propertyOrder" : 100,
      "items" : {
        "type" : "string"
      },
      "minItems" : 1,
      "type" : "array",
      "exampleValue" : ""
    },
    "distance" : {
      "title" : "Geofence Radius (km)",
      "description" : "Specifies the maximum distance, in kilometers, that a device can be from the
 specified trusted location(s).",
      "propertyOrder" : 200,
      "type" : "string",
      "exampleValue" : ""
    }
  },
  "required" : [ "locations", "distance" ]
}
```

delete

Usage:

```
am> delete DeviceGeofencing --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action DeviceGeofencing --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action DeviceGeofencing --realm Realm --actionName getCreatableTypes
```

listOutcomes

List the available outcomes for the node type.

Usage:

```
am> action DeviceGeofencing --realm Realm --body body --actionName listOutcomes
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "title" : "Some configuration of the node. This does not need to be complete against the
 configuration schema."
}
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action DeviceGeofencing --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query DeviceGeofencing --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read DeviceGeofencing --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update DeviceGeofencing --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "locations" : {
      "title" : "Trusted Locations",
      "description" : "Specify the latitude and longitude of trusted locations. Separate the values
 with a comma; for example, `-123.177201,49.164532`.",
      "propertyOrder" : 100,
      "items" : {
        "type" : "string"
      },
      "minItems" : 1,
      "type" : "array",
      "exampleValue" : ""
    },
    "distance" : {
      "title" : "Geofence Radius (km)",
      "description" : "Specifies the maximum distance, in kilometers, that a device can be from the
 specified trusted location(s).",
      "propertyOrder" : 200,
      "type" : "string",
      "exampleValue" : ""
    }
  },
  "required" : [ "locations", "distance" ]
}
```

DeviceIDService

Realm Operations

Resource path: `/realm-config/services/deviceIdService`

Resource version: `1.0`

create

Usage:

```
am> create DeviceIDService --realm Realm --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "deviceIdAttrName" : {
      "title" : "Profile Storage Attribute",
      "description" : "The user's attribute in which to store Device ID profiles.<br><br>The default
 attribute is added to the schema when you prepare a user store for use with OpenAM. If you want to
 use a different attribute, you must make sure to add it to your user store schema prior to enabling
 the Device ID authentication module. OpenAM must be able to write to the attribute.",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "deviceIdSettingsEncryptionScheme" : {
      "title" : "Device Profile Encryption Scheme",
      "description" : "Encryption scheme to use to secure device profiles stored on the
 server.<br><br>If enabled, each device profile is encrypted using a unique random secret key
 using the given strength of AES encryption in CBC mode with PKCS#5 padding. An HMAC-SHA of the
 given strength (truncated to half-size) is used to ensure integrity protection and authenticated
 encryption. The unique random key is encrypted with the given RSA key pair and stored with the device
 profile.<p><p><i>Note:</i> AES-256 may require installation of the JCE Unlimited Strength policy
 files.",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "deviceIdSettingsEncryptionKeystoreType" : {
      "title" : "Key Store Type",
      "description" : "Type of key store to load.<br><br><i>Note:</i> PKCS#11 key stores require
 hardware support such as a security device or smart card and is not available by default in most
 JVM installations.<p><p>See the <a href=\"https://docs.oracle.com/javase/8/docs/technotes/guides/
security/p11guide.html\" target=\"_blank\">JDK 8 PKCS#11 Reference Guide</a> for more details.",
      "propertyOrder" : 400,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
```

```
    },
    "deviceIdSettingsEncryptionKeystorePassword" : {
      "title" : "Key Store Password",
      "description" : "Password to unlock the key store. This password is encrypted when it is saved
 in the OpenAM configuration. You should modify the default value.",
      "propertyOrder" : 500,
      "required" : false,
      "type" : "string",
      "format" : "password",
      "exampleValue" : ""
    },
    "deviceIdSettingsEncryptionKeystoreKeyPairAlias" : {
      "title" : "Key-Pair Alias",
      "description" : "Alias of the certificate and private key in the key store. The private key is
 used to encrypt and decrypt device profiles.",
      "propertyOrder" : 600,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
    },
    "deviceIdSettingsEncryptionKeystore" : {
      "title" : "Encryption Key Store",
      "description" : "Path to the key store from which to load encryption keys.",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "deviceIdSettingsEncryptionKeystorePrivateKeyPassword" : {
      "title" : "Private Key Password",
      "description" : "Password to unlock the private key.",
      "propertyOrder" : 700,
      "required" : false,
      "type" : "string",
      "format" : "password",
      "exampleValue" : ""
    }
  }
}
```

delete

Usage:

```
am> delete DeviceIDService --realm Realm
```

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action DeviceIDService --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action DeviceIDService --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action DeviceIDService --realm Realm --actionName nextdescendents
```

read

Usage:

```
am> read DeviceIDService --realm Realm
```

update

Usage:

```
am> update DeviceIDService --realm Realm --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "deviceIdAttrName" : {
      "title" : "Profile Storage Attribute",
      "description" : "The user's attribute in which to store Device ID profiles.<br><br>The default
 attribute is added to the schema when you prepare a user store for use with OpenAM. If you want to
 use a different attribute, you must make sure to add it to your user store schema prior to enabling
 the Device ID authentication module. OpenAM must be able to write to the attribute.",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "deviceIdSettingsEncryptionScheme" : {
      "title" : "Device Profile Encryption Scheme",
      "description" : "Encryption scheme to use to secure device profiles stored on the
 server.<br><br>If enabled, each device profile is encrypted using a unique random secret key
 using the given strength of AES encryption in CBC mode with PKCS#5 padding. An HMAC-SHA of the
```

```
 given strength (truncated to half-size) is used to ensure integrity protection and authenticated
 encryption. The unique random key is encrypted with the given RSA key pair and stored with the device
 profile.<p><p><i>Note:</i> AES-256 may require installation of the JCE Unlimited Strength policy
 files.",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "deviceIdSettingsEncryptionKeystoreType" : {
      "title" : "Key Store Type",
      "description" : "Type of key store to load.<br><br><i>Note:</i> PKCS#11 key stores require
 hardware support such as a security device or smart card and is not available by default in most
 JVM installations.<p><p>See the <a href=\"https://docs.oracle.com/javase/8/docs/technotes/guides/
security/p11guide.html\" target=\"_blank\">JDK 8 PKCS#11 Reference Guide</a> for more details.",
      "propertyOrder" : 400,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "deviceIdSettingsEncryptionKeystorePassword" : {
      "title" : "Key Store Password",
      "description" : "Password to unlock the key store. This password is encrypted when it is saved
 in the OpenAM configuration. You should modify the default value.",
      "propertyOrder" : 500,
      "required" : false,
      "type" : "string",
      "format" : "password",
      "exampleValue" : ""
    },
    "deviceIdSettingsEncryptionKeystoreKeyPairAlias" : {
      "title" : "Key-Pair Alias",
      "description" : "Alias of the certificate and private key in the key store. The private key is
 used to encrypt and decrypt device profiles.",
      "propertyOrder" : 600,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
    },
    "deviceIdSettingsEncryptionKeystore" : {
      "title" : "Encryption Key Store",
      "description" : "Path to the key store from which to load encryption keys.",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "deviceIdSettingsEncryptionKeystorePrivateKeyPassword" : {
      "title" : "Private Key Password",
      "description" : "Password to unlock the private key.",
      "propertyOrder" : 700,
      "required" : false,
      "type" : "string",
      "format" : "password",
      "exampleValue" : ""
    }
  }
}
```

Global Operations

Resource path: `/global-config/services/deviceIdService`

Resource version: `1.0`

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action DeviceIDService --global --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action DeviceIDService --global --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action DeviceIDService --global --actionName nextdescendents
```

read

Usage:

```
am> read DeviceIDService --global
```

update

Usage:

```
am> update DeviceIDService --global --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "defaults" : {
      "properties" : {
        "deviceIdSettingsEncryptionKeystorePassword" : {
          "title" : "Key Store Password",
          "description" : "Password to unlock the key store. This password is encrypted when it is
 saved in the OpenAM configuration. You should modify the default value.",
          "propertyOrder" : 500,
          "required" : false,
          "type" : "string",
          "format" : "password",
          "exampleValue" : ""
        },
        "deviceIdSettingsEncryptionKeystorePrivateKeyPassword" : {
          "title" : "Private Key Password",
          "description" : "Password to unlock the private key.",
          "propertyOrder" : 700,
          "required" : false,
          "type" : "string",
          "format" : "password",
          "exampleValue" : ""
        },
        "deviceIdSettingsEncryptionKeystore" : {
          "title" : "Encryption Key Store",
          "description" : "Path to the key store from which to load encryption keys.",
          "propertyOrder" : 300,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "deviceIdAttrName" : {
          "title" : "Profile Storage Attribute",
          "description" : "The user's attribute in which to store Device ID profiles.<br><br>The
 default attribute is added to the schema when you prepare a user store for use with OpenAM. If you
 want to use a different attribute, you must make sure to add it to your user store schema prior to
 enabling the Device ID authentication module. OpenAM must be able to write to the attribute.",
          "propertyOrder" : 100,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "deviceIdSettingsEncryptionKeystoreType" : {
          "title" : "Key Store Type",
          "description" : "Type of key store to load.<br><br><i>Note:</i> PKCS#11 key stores require
 hardware support such as a security device or smart card and is not available by default in most
 JVM installations.<p><p>See the <a href=\"https://docs.oracle.com/javase/8/docs/technotes/guides/
security/p11guide.html\" target=\"_blank\">JDK 8 PKCS#11 Reference Guide</a> for more details.",
          "propertyOrder" : 400,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "deviceIdSettingsEncryptionKeystoreKeyPairAlias" : {
```

```
          "title" : "Key-Pair Alias",
          "description" : "Alias of the certificate and private key in the key store. The private key
 is used to encrypt and decrypt device profiles.",
          "propertyOrder" : 600,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "deviceIdSettingsEncryptionScheme" : {
          "title" : "Device Profile Encryption Scheme",
          "description" : "Encryption scheme to use to secure device profiles stored on the
 server.<br><br>If enabled, each device profile is encrypted using a unique random secret key
 using the given strength of AES encryption in CBC mode with PKCS#5 padding. An HMAC-SHA of the
 given strength (truncated to half-size) is used to ensure integrity protection and authenticated
 encryption. The unique random key is encrypted with the given RSA key pair and stored with the device
 profile.<p><p><i>Note:</i> AES-256 may require installation of the JCE Unlimited Strength policy
 files.",
          "propertyOrder" : 200,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      },
      "type" : "object",
      "title" : "Realm Defaults"
    }
  }
}
```

DeviceIdMatchModule

Realm Operations

Resource path: `/realm-config/authentication/modules/deviceidmatch`

Resource version: `1.0`

create

Usage:

```
am> create DeviceIdMatchModule --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "serverScript" : {
      "title" : "Server-side Script",
      "description" : "The server-side script to execute.<br><br>This script will be run on
 the server, subsequent to any client script having returned. It can be written in the selected
 language.",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "clientScriptEnabled" : {
      "title" : "Client-side Script Enabled",
      "description" : "Enable this setting if the client-side script should be executed.",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "clientScript" : {
      "title" : "Client-side Script",
      "description" : "The client-side script.",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "authenticationLevel" : {
      "title" : "Authentication Level",
      "description" : "The authentication level associated with the authentication module.<br><br>Each
 authentication module has an authentication level that can be used to indicate the level of security
 associated with the module; 0 is the lowest (and the default).",
      "propertyOrder" : 400,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    }
  }
}
```

delete

Usage:

```
am> delete DeviceIdMatchModule --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action DeviceIdMatchModule --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action DeviceIdMatchModule --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action DeviceIdMatchModule --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query DeviceIdMatchModule --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read DeviceIdMatchModule --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update DeviceIdMatchModule --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "serverScript" : {
      "title" : "Server-side Script",
      "description" : "The server-side script to execute.<br><br>This script will be run on
 the server, subsequent to any client script having returned. It can be written in the selected
 language.",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "clientScriptEnabled" : {
      "title" : "Client-side Script Enabled",
      "description" : "Enable this setting if the client-side script should be executed.",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "clientScript" : {
      "title" : "Client-side Script",
      "description" : "The client-side script.",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "authenticationLevel" : {
      "title" : "Authentication Level",
      "description" : "The authentication level associated with the authentication module.<br><br>Each
 authentication module has an authentication level that can be used to indicate the level of security
 associated with the module; 0 is the lowest (and the default).",
      "propertyOrder" : 400,
```

```
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    }
  }
}
```

Global Operations

Resource path: `/global-config/authentication/modules/deviceidmatch`

Resource version: `1.0`

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action DeviceIdMatchModule --global --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action DeviceIdMatchModule --global --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action DeviceIdMatchModule --global --actionName nextdescendents
```

read

Usage:

```
am> read DeviceIdMatchModule --global
```

update

Usage:

```
am> update DeviceIdMatchModule --global --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "defaults" : {
      "properties" : {
        "serverScript" : {
          "title" : "Server-side Script",
          "description" : "The server-side script to execute.<br><br>This script will be run on
 the server, subsequent to any client script having returned. It can be written in the selected
 language.",
          "propertyOrder" : 300,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "clientScript" : {
          "title" : "Client-side Script",
          "description" : "The client-side script.",
          "propertyOrder" : 200,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "clientScriptEnabled" : {
          "title" : "Client-side Script Enabled",
          "description" : "Enable this setting if the client-side script should be executed.",
          "propertyOrder" : 100,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "authenticationLevel" : {
          "title" : "Authentication Level",
          "description" : "The authentication level associated with the authentication
 module.<br><br>Each authentication module has an authentication level that can be used to indicate
 the level of security associated with the module; 0 is the lowest (and the default).",
          "propertyOrder" : 400,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        }
      },
      "type" : "object",
      "title" : "Realm Defaults"
    }
  }
}
```

DeviceIdSaveModule

Realm Operations

Resource path: `/realm-config/authentication/modules/deviceidsave`

Resource version: `1.0`

create

Usage:

```
am> create DeviceIdSaveModule --realm Realm --id id --body body
```

Parameters:

`--id`

The unique identifier for the resource.

`--body`

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "authenticationLevel" : {
      "title" : "Authentication Level",
      "description" : "The authentication level associated with the authentication module.<br><br>Each
 authentication module has an authentication level that can be used to indicate the level of security
 associated with the module; 0 is the lowest (and the default).",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "maxProfilesAllowed" : {
      "title" : "Maximum stored profile quantity",
      "description" : "No more than specified profiles quantity will be stored in user record",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "autoStoreProfiles" : {
      "title" : "Automatically store new profiles",
      "description" : "Select this checkbox to assume user consent to store every new
 profile<br><br>If this checkbox is selected user won't be prompted for storing new profiles. After
 successful OTP confirmation profile will be stored automatically.",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    }
  }
}
```

delete

Usage:

```
am> delete DeviceIdSaveModule --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action DeviceIdSaveModule --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action DeviceIdSaveModule --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action DeviceIdSaveModule --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query DeviceIdSaveModule --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read DeviceIdSaveModule --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update DeviceIdSaveModule --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "authenticationLevel" : {
      "title" : "Authentication Level",
      "description" : "The authentication level associated with the authentication module.<br><br>Each
 authentication module has an authentication level that can be used to indicate the level of security
 associated with the module; 0 is the lowest (and the default).",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "maxProfilesAllowed" : {
      "title" : "Maximum stored profile quantity",
      "description" : "No more than specified profiles quantity will be stored in user record",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "autoStoreProfiles" : {
      "title" : "Automatically store new profiles",
      "description" : "Select this checkbox to assume user consent to store every new
 profile<br><br>If this checkbox is selected user won't be prompted for storing new profiles. After
 successful OTP confirmation profile will be stored automatically.",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    }
  }
}
```

Global Operations

Resource path: `/global-config/authentication/modules/deviceidsave`

Resource version: `1.0`

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action DeviceIdSaveModule --global --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action DeviceIdSaveModule --global --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action DeviceIdSaveModule --global --actionName nextdescendents
```

read

Usage:

```
am> read DeviceIdSaveModule --global
```

update

Usage:

```
am> update DeviceIdSaveModule --global --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "defaults" : {
      "properties" : {
        "maxProfilesAllowed" : {
          "title" : "Maximum stored profile quantity",
          "description" : "No more than specified profiles quantity will be stored in user record",
          "propertyOrder" : 200,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "autoStoreProfiles" : {
```

```
          "title" : "Automatically store new profiles",
          "description" : "Select this checkbox to assume user consent to store every new
 profile<br><br>If this checkbox is selected user won't be prompted for storing new profiles. After
 successful OTP confirmation profile will be stored automatically.",
          "propertyOrder" : 100,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "authenticationLevel" : {
          "title" : "Authentication Level",
          "description" : "The authentication level associated with the authentication
 module.<br><br>Each authentication module has an authentication level that can be used to indicate
 the level of security associated with the module; 0 is the lowest (and the default).",
          "propertyOrder" : 300,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        }
      },
      "type" : "object",
      "title" : "Realm Defaults"
    }
  }
}
```

DeviceLocationMatch

Realm Operations

Resource path: `/realm-config/authentication/authenticationtrees/nodes/DeviceLocationMatchNode`

Resource version: `1.0`

create

Usage:

```
am> create DeviceLocationMatch --realm Realm --id id --body body
```

Parameters:

`--id`

The unique identifier for the resource.

`--body`

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "distance" : {
      "title" : "Maximum Radius (km)",
      "description" : "Specifies the maximum distance, in kilometers, that a device can be from a
 previously saved location.",
      "propertyOrder" : 100,
      "type" : "string",
      "exampleValue" : ""
    }
  },
  "required" : [ "distance" ]
}
```

delete

Usage:

```
am> delete DeviceLocationMatch --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action DeviceLocationMatch --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action DeviceLocationMatch --realm Realm --actionName getCreatableTypes
```

listOutcomes

List the available outcomes for the node type.

Usage:

```
am> action DeviceLocationMatch --realm Realm --body body --actionName listOutcomes
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "title" : "Some configuration of the node. This does not need to be complete against the
 configuration schema."
}
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action DeviceLocationMatch --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query DeviceLocationMatch --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read DeviceLocationMatch --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update DeviceLocationMatch --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "distance" : {
      "title" : "Maximum Radius (km)",
      "description" : "Specifies the maximum distance, in kilometers, that a device can be from a
 previously saved location.",
      "propertyOrder" : 100,
      "type" : "string",
      "exampleValue" : ""
    }
  },
  "required" : [ "distance" ]
}
```

DeviceMatch

Realm Operations

Resource path: `/realm-config/authentication/authenticationtrees/nodes/DeviceMatchNode`

Resource version: `1.0`

create

Usage:

```
am> create DeviceMatch --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "expiration" : {
      "title" : "Expiration",
      "description" : "Specify the number of days until profile expiration. Expired profiles will not
 match.",
      "propertyOrder" : 200,
      "type" : "integer",
      "exampleValue" : ""
    },
    "acceptableVariance" : {
      "title" : "Acceptable Variance",
      "description" : "Specify the maximum amount of device attribute differences that is still
 acceptable for a match.",
      "propertyOrder" : 100,
      "type" : "integer",
      "exampleValue" : ""
    },
    "script" : {
      "title" : "Custom Matching Script",
      "description" : "Decision Node Script",
      "propertyOrder" : 400,
      "type" : "string",
      "exampleValue" : ""
    },
    "useScript" : {
      "title" : "Use Custom Matching Script",
      "description" : "Use a custom script for matching device profiles. When enabled, the Acceptable
 Variance and Expiration properties are ignored. The script's type has to be: Decision Node Script.",
      "propertyOrder" : 300,
      "type" : "boolean",
      "exampleValue" : ""
    }
  },
  "required" : [ "acceptableVariance", "useScript", "script", "expiration" ]
}
```

delete

Usage:

```
am> delete DeviceMatch --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action DeviceMatch --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action DeviceMatch --realm Realm --actionName getCreatableTypes
```

listOutcomes

List the available outcomes for the node type.

Usage:

```
am> action DeviceMatch --realm Realm --body body --actionName listOutcomes
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "title" : "Some configuration of the node. This does not need to be complete against the
 configuration schema."
}
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action DeviceMatch --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query DeviceMatch --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read DeviceMatch --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update DeviceMatch --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "expiration" : {
      "title" : "Expiration",
      "description" : "Specify the number of days until profile expiration. Expired profiles will not
 match.",
      "propertyOrder" : 200,
      "type" : "integer",
      "exampleValue" : ""
    },
    "acceptableVariance" : {
      "title" : "Acceptable Variance",
      "description" : "Specify the maximum amount of device attribute differences that is still
 acceptable for a match.",
      "propertyOrder" : 100,
      "type" : "integer",
      "exampleValue" : ""
```

```
    },
    "script" : {
      "title" : "Custom Matching Script",
      "description" : "Decision Node Script",
      "propertyOrder" : 400,
      "type" : "string",
      "exampleValue" : ""
    },
    "useScript" : {
      "title" : "Use Custom Matching Script",
      "description" : "Use a custom script for matching device profiles. When enabled, the Acceptable
 Variance and Expiration properties are ignored. The script's type has to be: Decision Node Script.",
      "propertyOrder" : 300,
      "type" : "boolean",
      "exampleValue" : ""
    }
  },
  "required" : [ "acceptableVariance", "useScript", "script", "expiration" ]
}
```

DeviceProfile

Realm Operations

The device profile service is responsible for exposing functions to change the collection of User devices. The supported methods are update, delete, query

Resource path: `/users/{user}/devices/profile`

Resource version: `1.0`

delete

Delete user device

Usage:

```
am> delete DeviceProfile --realm Realm --id id --user user
```

Parameters:

`--id`

The unique identifier for the resource.

`--user`

The device profile service is responsible for exposing functions to change the collection of User devices. The supported methods are update, delete, query

query

Query the user devices

Usage:

```
am> query DeviceProfile --realm Realm --filter filter --user user
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all. Fields that can be queried: [*]

--user

The device profile service is responsible for exposing functions to change the collection of User devices. The supported methods are update, delete, query

update

Update an existing user device alias

Usage:

```
am> update DeviceProfile --realm Realm --id id --body body --user user
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "$schema" : "http://json-schema.org/draft-04/schema#",
  "description" : "User devices schema that is used for device profile",
  "type" : "object",
  "title" : "User devices schema",
  "properties" : {
    "identifier" : {
      "type" : "string",
      "title" : "Identifier",
      "description" : "The unique identifier of the device"
    },
    "alias" : {
      "type" : "string",
      "title" : "Device alias name",
      "description" : "The alias name of user device"
```

```
    },
    "lastSelectedDate" : {
      "type" : "string",
      "title" : "Last selected date",
      "description" : "Date when the device was selected last time"
    },
    "metadata" : {
      "type" : "object",
      "title" : "Device Metadata",
      "description" : "The JSON representation of device metadata"
    },
    "location" : {
      "type" : "object",
      "title" : "Device Location",
      "description" : "The current device location",
      "properties" : {
        "longitude" : {
          "type" : "number",
          "title" : "Location latitude",
          "description" : "The location latitude"
        },
        "latitude" : {
          "type" : "number",
          "title" : "Location longitude",
          "description" : "The location longitude"
        }
      }
    }
  }
}
```

--user

The device profile service is responsible for exposing functions to change the collection of User devices. The supported methods are update, delete, query

DeviceProfileCollector

Realm Operations

Resource path: `/realm-config/authentication/authenticationtrees/nodes/DeviceProfileCollectorNode`

Resource version: `1.0`

create

Usage:

```
am> create DeviceProfileCollector --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "deviceMetadata" : {
      "title" : "Collect Device Metadata",
      "description" : "Instructs the client to collect device metadata.",
      "propertyOrder" : 200,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "deviceLocation" : {
      "title" : "Collect Device Location",
      "description" : "Instructs the client to collect device location.",
      "propertyOrder" : 300,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "message" : {
      "title" : "Message",
      "description" : "Optional message to display to the user when capturing device information.
 Enter a locale in the KEY field, for example `en-us`, and the localized message as the VALUE.",
      "propertyOrder" : 400,
      "patternProperties" : {
        ".*" : {
          "type" : "string"
        }
      },
      "type" : "object",
      "exampleValue" : ""
    },
    "maximumSize" : {
      "title" : "Maximum Profile Size (KB)",
      "description" : "Specify the maximum accepted size for a device profile in kilobytes. If the
 returned profile size exceeds this maximum the authentication will fail. Note that larger profiles
 can impact performance.",
      "propertyOrder" : 100,
      "type" : "string",
      "exampleValue" : ""
    }
  },
  "required" : [ "deviceLocation", "deviceMetadata", "message", "maximumSize" ]
}
```

delete

Usage:

```
am> delete DeviceProfileCollector --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action DeviceProfileCollector --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action DeviceProfileCollector --realm Realm --actionName getCreatableTypes
```

listOutcomes

List the available outcomes for the node type.

Usage:

```
am> action DeviceProfileCollector --realm Realm --body body --actionName listOutcomes
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "title" : "Some configuration of the node. This does not need to be complete against the
 configuration schema."
}
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action DeviceProfileCollector --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query DeviceProfileCollector --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read DeviceProfileCollector --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update DeviceProfileCollector --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
```

```
  "properties" : {
    "deviceMetadata" : {
      "title" : "Collect Device Metadata",
      "description" : "Instructs the client to collect device metadata.",
      "propertyOrder" : 200,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "deviceLocation" : {
      "title" : "Collect Device Location",
      "description" : "Instructs the client to collect device location.",
      "propertyOrder" : 300,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "message" : {
      "title" : "Message",
      "description" : "Optional message to display to the user when capturing device information.
 Enter a locale in the KEY field, for example `en-us`, and the localized message as the VALUE.",
      "propertyOrder" : 400,
      "patternProperties" : {
        ".*" : {
          "type" : "string"
        }
      },
      "type" : "object",
      "exampleValue" : ""
    },
    "maximumSize" : {
      "title" : "Maximum Profile Size (KB)",
      "description" : "Specify the maximum accepted size for a device profile in kilobytes. If the
 returned profile size exceeds this maximum the authentication will fail. Note that larger profiles
 can impact performance.",
      "propertyOrder" : 100,
      "type" : "string",
      "exampleValue" : ""
    }
  },
  "required" : [ "deviceLocation", "deviceMetadata", "message", "maximumSize" ]
}
```

DeviceProfileSave

Realm Operations

Resource path: `/realm-config/authentication/authenticationtrees/nodes/DeviceSaveNode`

Resource version: `1.0`

create

Usage:

```
am> create DeviceProfileSave --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "maxSavedProfiles" : {
      "title" : "Maximum Saved Profiles",
      "description" : "Specify the maximum number of device profiles to save in a user's profile. When
 the maximum is reached, saving a new profile replaces the least-recently used profile.",
      "propertyOrder" : 200,
      "type" : "integer",
      "exampleValue" : ""
    },
    "variableName" : {
      "title" : "Device Name Variable",
      "description" : "Specify an existing variable name, in shared state, that contains the value to
 use as this device's name.",
      "propertyOrder" : 100,
      "type" : "string",
      "exampleValue" : ""
    },
    "saveDeviceMetadata" : {
      "title" : "Save Device Metadata",
      "description" : "Specify whether device metadata should be saved.",
      "propertyOrder" : 300,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "saveDeviceLocation" : {
      "title" : "Save Device Location",
      "description" : "Specify whether device location should be saved.",
      "propertyOrder" : 400,
      "type" : "boolean",
      "exampleValue" : ""
    }
  },
  "required" : [ "saveDeviceMetadata", "variableName", "maxSavedProfiles", "saveDeviceLocation" ]
}
```

delete

Usage:

```
am> delete DeviceProfileSave --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action DeviceProfileSave --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action DeviceProfileSave --realm Realm --actionName getCreatableTypes
```

listOutcomes

List the available outcomes for the node type.

Usage:

```
am> action DeviceProfileSave --realm Realm --body body --actionName listOutcomes
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "title" : "Some configuration of the node. This does not need to be complete against the
 configuration schema."
}
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action DeviceProfileSave --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query DeviceProfileSave --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read DeviceProfileSave --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update DeviceProfileSave --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
```

```
  "properties" : {
    "maxSavedProfiles" : {
      "title" : "Maximum Saved Profiles",
      "description" : "Specify the maximum number of device profiles to save in a user's profile. When
 the maximum is reached, saving a new profile replaces the least-recently used profile.",
      "propertyOrder" : 200,
      "type" : "integer",
      "exampleValue" : ""
    },
    "variableName" : {
      "title" : "Device Name Variable",
      "description" : "Specify an existing variable name, in shared state, that contains the value to
 use as this device's name.",
      "propertyOrder" : 100,
      "type" : "string",
      "exampleValue" : ""
    },
    "saveDeviceMetadata" : {
      "title" : "Save Device Metadata",
      "description" : "Specify whether device metadata should be saved.",
      "propertyOrder" : 300,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "saveDeviceLocation" : {
      "title" : "Save Device Location",
      "description" : "Specify whether device location should be saved.",
      "propertyOrder" : 400,
      "type" : "boolean",
      "exampleValue" : ""
    }
  },
  "required" : [ "saveDeviceMetadata", "variableName", "maxSavedProfiles", "saveDeviceLocation" ]
}
```

DeviceProfilesService

Realm Operations

Resource path: `/realm-config/services/deviceProfilesService`

Resource version: `1.0`

create

Usage:

```
am> create DeviceProfilesService --realm Realm --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "deviceProfilesSettingsEncryptionKeystore" : {
      "title" : "Encryption Key Store",
      "description" : "Path to the key store from which to load encryption keys.",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "deviceProfilesSettingsEncryptionKeystoreKeyPairAlias" : {
      "title" : "Key-Pair Alias",
      "description" : "Alias of the certificate and private key in the key store. The private key is
 used to encrypt and decrypt device profiles.",
      "propertyOrder" : 600,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
    },
    "deviceProfilesSettingsEncryptionKeystoreType" : {
      "title" : "Key Store Type",
      "description" : "Type of key store to load.<br><br><i>Note:</i> PKCS#11 key stores require
 hardware support such as a security device or smart card and is not available by default in most
 JVM installations.<p><p>See the <a href=\"https://docs.oracle.com/javase/8/docs/technotes/guides/
security/p11guide.html\" target=\"_blank\">JDK 8 PKCS#11 Reference Guide</a> for more details.",
      "propertyOrder" : 400,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "deviceProfilesSettingsEncryptionKeystorePrivateKeyPassword" : {
      "title" : "Private Key Password",
      "description" : "Password to unlock the private key.",
      "propertyOrder" : 700,
      "required" : false,
      "type" : "string",
      "format" : "password",
      "exampleValue" : ""
    },
    "deviceProfilesSettingsEncryptionKeystorePassword" : {
      "title" : "Key Store Password",
      "description" : "Password to unlock the key store. This password is encrypted when it is saved
 in the OpenAM configuration. You should modify the default value.",
      "propertyOrder" : 500,
      "required" : false,
      "type" : "string",
      "format" : "password",
      "exampleValue" : ""
    },
    "deviceProfilesSettingsEncryptionScheme" : {
      "title" : "Device Profile Encryption Scheme",
      "description" : "Encryption scheme to use to secure device profiles stored on the
 server.<br><br>If enabled, each device profile is encrypted using a unique random secret key
 using the given strength of AES encryption in CBC mode with PKCS#5 padding. An HMAC-SHA of the
```

```
 given strength (truncated to half-size) is used to ensure integrity protection and authenticated
 encryption. The unique random key is encrypted with the given RSA key pair and stored with the device
 profile.<p><p><i>Note:</i> AES-256 may require installation of the JCE Unlimited Strength policy
 files.",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "deviceProfilesAttrName" : {
      "title" : "Profile Storage Attribute",
      "description" : "The user's attribute in which to store Device profiles.<br><br>The default
 attribute is added to the schema when you prepare a user store for use with OpenAM. If you want to
 use a different attribute, you must make sure to add it to your user store schema prior to enabling
 the Device Profiles authentication module. OpenAM must be able to write to the attribute.",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
```

delete

Usage:

```
am> delete DeviceProfilesService --realm Realm
```

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action DeviceProfilesService --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action DeviceProfilesService --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action DeviceProfilesService --realm Realm --actionName nextdescendents
```

read

Usage:

```
am> read DeviceProfilesService --realm Realm
```

update

Usage:

```
am> update DeviceProfilesService --realm Realm --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "deviceProfilesSettingsEncryptionKeystore" : {
      "title" : "Encryption Key Store",
      "description" : "Path to the key store from which to load encryption keys.",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "deviceProfilesSettingsEncryptionKeystoreKeyPairAlias" : {
      "title" : "Key-Pair Alias",
      "description" : "Alias of the certificate and private key in the key store. The private key is
 used to encrypt and decrypt device profiles.",
      "propertyOrder" : 600,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
    },
    "deviceProfilesSettingsEncryptionKeystoreType" : {
      "title" : "Key Store Type",
      "description" : "Type of key store to load.<br><br><i>Note:</i> PKCS#11 key stores require
 hardware support such as a security device or smart card and is not available by default in most
 JVM installations.<p><p>See the <a href=\"https://docs.oracle.com/javase/8/docs/technotes/guides/
security/p11guide.html\" target=\"_blank\">JDK 8 PKCS#11 Reference Guide</a> for more details.",
      "propertyOrder" : 400,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "deviceProfilesSettingsEncryptionKeystorePrivateKeyPassword" : {
      "title" : "Private Key Password",
      "description" : "Password to unlock the private key.",
      "propertyOrder" : 700,
      "required" : false,
      "type" : "string",
```

```
      "format" : "password",
      "exampleValue" : ""
    },
    "deviceProfilesSettingsEncryptionKeystorePassword" : {
      "title" : "Key Store Password",
      "description" : "Password to unlock the key store. This password is encrypted when it is saved
 in the OpenAM configuration. You should modify the default value.",
      "propertyOrder" : 500,
      "required" : false,
      "type" : "string",
      "format" : "password",
      "exampleValue" : ""
    },
    "deviceProfilesSettingsEncryptionScheme" : {
      "title" : "Device Profile Encryption Scheme",
      "description" : "Encryption scheme to use to secure device profiles stored on the
 server.<br><br>If enabled, each device profile is encrypted using a unique random secret key
 using the given strength of AES encryption in CBC mode with PKCS#5 padding. An HMAC-SHA of the
 given strength (truncated to half-size) is used to ensure integrity protection and authenticated
 encryption. The unique random key is encrypted with the given RSA key pair and stored with the device
 profile.<p><p><i>Note:</i> AES-256 may require installation of the JCE Unlimited Strength policy
 files.",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "deviceProfilesAttrName" : {
      "title" : "Profile Storage Attribute",
      "description" : "The user's attribute in which to store Device profiles.<br><br>The default
 attribute is added to the schema when you prepare a user store for use with OpenAM. If you want to
 use a different attribute, you must make sure to add it to your user store schema prior to enabling
 the Device Profiles authentication module. OpenAM must be able to write to the attribute.",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
```

Global Operations

Resource path: `/global-config/services/deviceProfilesService`

Resource version: `1.0`

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action DeviceProfilesService --global --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action DeviceProfilesService --global --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action DeviceProfilesService --global --actionName nextdescendents
```

read

Usage:

```
am> read DeviceProfilesService --global
```

update

Usage:

```
am> update DeviceProfilesService --global --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "defaults" : {
      "properties" : {
        "deviceProfilesAttrName" : {
          "title" : "Profile Storage Attribute",
          "description" : "The user's attribute in which to store Device profiles.<br><br>The default
 attribute is added to the schema when you prepare a user store for use with OpenAM. If you want to
 use a different attribute, you must make sure to add it to your user store schema prior to enabling
 the Device Profiles authentication module. OpenAM must be able to write to the attribute.",
          "propertyOrder" : 100,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "deviceProfilesSettingsEncryptionKeystoreType" : {
          "title" : "Key Store Type",
```

```
          "description" : "Type of key store to load.<br><br><i>Note:</i> PKCS#11 key stores require
 hardware support such as a security device or smart card and is not available by default in most
 JVM installations.<p><p>See the <a href=\"https://docs.oracle.com/javase/8/docs/technotes/guides/
security/p11guide.html\" target=\"_blank\">JDK 8 PKCS#11 Reference Guide</a> for more details.",
          "propertyOrder" : 400,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "deviceProfilesSettingsEncryptionScheme" : {
          "title" : "Device Profile Encryption Scheme",
          "description" : "Encryption scheme to use to secure device profiles stored on the
 server.<br><br>If enabled, each device profile is encrypted using a unique random secret key
 using the given strength of AES encryption in CBC mode with PKCS#5 padding. An HMAC-SHA of the
 given strength (truncated to half-size) is used to ensure integrity protection and authenticated
 encryption. The unique random key is encrypted with the given RSA key pair and stored with the device
 profile.<p><p><i>Note:</i> AES-256 may require installation of the JCE Unlimited Strength policy
 files.",
          "propertyOrder" : 200,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "deviceProfilesSettingsEncryptionKeystorePrivateKeyPassword" : {
          "title" : "Private Key Password",
          "description" : "Password to unlock the private key.",
          "propertyOrder" : 700,
          "required" : false,
          "type" : "string",
          "format" : "password",
          "exampleValue" : ""
        },
        "deviceProfilesSettingsEncryptionKeystoreKeyPairAlias" : {
          "title" : "Key-Pair Alias",
          "description" : "Alias of the certificate and private key in the key store. The private key
 is used to encrypt and decrypt device profiles.",
          "propertyOrder" : 600,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "deviceProfilesSettingsEncryptionKeystorePassword" : {
          "title" : "Key Store Password",
          "description" : "Password to unlock the key store. This password is encrypted when it is
 saved in the OpenAM configuration. You should modify the default value.",
          "propertyOrder" : 500,
          "required" : false,
          "type" : "string",
          "format" : "password",
          "exampleValue" : ""
        },
        "deviceProfilesSettingsEncryptionKeystore" : {
          "title" : "Encryption Key Store",
          "description" : "Path to the key store from which to load encryption keys.",
          "propertyOrder" : 300,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
```

```
      },
      "type" : "object",
      "title" : "Realm Defaults"
    }
  }
}
```

DeviceTamperingVerification

Realm Operations

Resource path: `/realm-config/authentication/authenticationtrees/nodes/DeviceTamperingVerificationNode`

Resource version: `1.0`

create

Usage:

```
am> create DeviceTamperingVerification --realm Realm --id id --body body
```

Parameters:

`--id`

The unique identifier for the resource.

`--body`

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "score" : {
      "title" : "Score Threshold",
      "description" : "Specifies the score threshold for determining if a device is jailbroken or
 rooted. Jailbreak scores received from the client will be between 0 and 1. The higher the score, the
 more likely the device is jailbroken (Emulators will score a 1).",
      "propertyOrder" : 100,
      "type" : "string",
      "exampleValue" : ""
    }
  },
  "required" : [ "score" ]
}
```

delete

Usage:

```
am> delete DeviceTamperingVerification --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action DeviceTamperingVerification --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action DeviceTamperingVerification --realm Realm --actionName getCreatableTypes
```

listOutcomes

List the available outcomes for the node type.

Usage:

```
am> action DeviceTamperingVerification --realm Realm --body body --actionName listOutcomes
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "title" : "Some configuration of the node. This does not need to be complete against the
 configuration schema."
}
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action DeviceTamperingVerification --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query DeviceTamperingVerification --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read DeviceTamperingVerification --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update DeviceTamperingVerification --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "score" : {
      "title" : "Score Threshold",
      "description" : "Specifies the score threshold for determining if a device is jailbroken or
 rooted. Jailbreak scores received from the client will be between 0 and 1. The higher the score, the
 more likely the device is jailbroken (Emulators will score a 1).",
      "propertyOrder" : 100,
      "type" : "string",
      "exampleValue" : ""
    }
  },
  "required" : [ "score" ]
}
```

DirectoryConfiguration

Global Operations

Connection details for directory server(s).

Resource path: `/global-config/servers/{serverName}/properties/directoryConfiguration`

Resource version: `1.0`

read

Usage:

```
am> read DirectoryConfiguration --global --serverName serverName
```

Parameters:

`--serverName`

Connection details for directory server(s).

update

Usage:

```
am> update DirectoryConfiguration --global --serverName serverName --body body
```

Parameters:

`--serverName`

Connection details for directory server(s).

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "directoryConfiguration" : {
      "type" : "object",
      "title" : "Directory Configuration",
      "propertyOrder" : 0,
      "properties" : {
        "minConnectionPool" : {
          "title" : "Minimum Connection Pool",
          "propertyOrder" : 0,
          "type" : "number"
        },
        "maxConnectionPool" : {
          "title" : "Maximum Connection Pool",
          "propertyOrder" : 1,
          "type" : "number"
        },
        "bindDn" : {
          "title" : "Bind DN",
          "propertyOrder" : 2,
          "type" : "string"
        },
        "bindPassword" : {
          "title" : "Bind Password",
          "propertyOrder" : 3,
          "type" : "string",
          "format" : "password"
        }
      }
    },
    "directoryServers" : {
      "type" : "array",
      "title" : "Server",
      "propertyOrder" : 1,
      "items" : {
        "type" : "object",
        "required" : [ "serverName", "hostName", "portNumber", "connectionType" ],
        "properties" : {
          "serverName" : {
            "title" : "Name",
            "type" : "string",
            "propertyOrder" : 0
          },
          "hostName" : {
            "title" : "Host Name",
            "type" : "string",
            "propertyOrder" : 1
          },
          "portNumber" : {
            "title" : "Port Number",
            "type" : "string",
            "propertyOrder" : 2
          },
          "connectionType" : {
```

```
            "type" : "string",
            "enum" : [ "SIMPLE", "SSL" ],
            "options" : {
              "enum_titles" : [ "SIMPLE", "SSL" ]
            },
            "title" : "Connection Type",
            "propertyOrder" : 3
          }
        }
      }
    }
  }
}
```

DisplayUsername

Realm Operations

Resource path: `/realm-config/authentication/authenticationtrees/nodes/DisplayUserNameNode`

Resource version: `1.0`

create

Usage:

```
am> create DisplayUsername --realm Realm --id id --body body
```

Parameters:

`--id`

The unique identifier for the resource.

`--body`

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "userName" : {
      "title" : "User Name",
      "description" : "The attribute used to identify the the user name in IDM.",
      "propertyOrder" : 100,
      "type" : "string",
      "exampleValue" : ""
    },
    "identityAttribute" : {
      "title" : "Identity Attribute",
      "description" : "The attribute used to identify the the object in IDM.",
      "propertyOrder" : 200,
      "type" : "string",
      "exampleValue" : ""
    }
  },
  "required" : [ "identityAttribute", "userName" ]
}
```

delete

Usage:

```
am> delete DisplayUsername --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action DisplayUsername --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action DisplayUsername --realm Realm --actionName getCreatableTypes
```

listOutcomes

List the available outcomes for the node type.

Usage:

```
am> action DisplayUsername --realm Realm --body body --actionName listOutcomes
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "title" : "Some configuration of the node. This does not need to be complete against the
 configuration schema."
}
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action DisplayUsername --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query DisplayUsername --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read DisplayUsername --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update DisplayUsername --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "userName" : {
      "title" : "User Name",
      "description" : "The attribute used to identify the the user name in IDM.",
      "propertyOrder" : 100,
      "type" : "string",
      "exampleValue" : ""
    },
    "identityAttribute" : {
      "title" : "Identity Attribute",
      "description" : "The attribute used to identify the the object in IDM.",
      "propertyOrder" : 200,
      "type" : "string",
      "exampleValue" : ""
    }
  },
  "required" : [ "identityAttribute", "userName" ]
}
```

ElasticSearch

Realm Operations

Resource path: `/realm-config/services/audit/Elasticsearch`

Resource version: `1.0`

create

Usage:

```
am> create ElasticSearch --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "elasticsearchBuffering" : {
      "type" : "object",
      "title" : "Buffering",
      "propertyOrder" : 4,
      "properties" : {
        "bufferingEnabled" : {
          "title" : "Buffering Enabled",
          "description" : "",
          "propertyOrder" : 5700,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "maxEvents" : {
          "title" : "Queue Capacity",
          "description" : "Maximum number of audit logs in the batch queue. Additional audit events
 are dropped.",
          "propertyOrder" : 5900,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "writeInterval" : {
          "title" : "Write interval (in milliseconds)",
          "description" : "Specifies the interval in milliseconds at which buffered events are written
 to Elasticsearch.",
          "propertyOrder" : 6000,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "batchSize" : {
          "title" : "Batch Size",
          "description" : "Maximum number of events that can be buffered (default: 10000)",
          "propertyOrder" : 5800,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        }
      }
    },
    "elasticsearchConfig" : {
      "type" : "object",
      "title" : "Elasticsearch Configuration",
      "propertyOrder" : 2,
      "properties" : {
```

```
       "host" : {
         "title" : "Server Hostname",
         "description" : "Host name or IP address of the Elasticsearch server.",
         "propertyOrder" : 5100,
         "required" : true,
         "type" : "string",
         "exampleValue" : ""
       },
       "sslEnabled" : {
         "title" : "SSL Enabled",
         "description" : "Specifies whether SSL is configured on the Elasticsearch server.<p><p>If
SSL is enabled, be sure to import the CA certificate used to sign Elasticsearch node certificates
into the Java keystore on the host that runs OpenAM before attempting to log audit events to
Elasticsearch.",
         "propertyOrder" : 5300,
         "required" : true,
         "type" : "boolean",
         "exampleValue" : ""
       },
       "port" : {
         "title" : "Server Port",
         "description" : "Specifies the port number used to access Elasticsearch's REST API.",
         "propertyOrder" : 5200,
         "required" : true,
         "type" : "integer",
         "exampleValue" : ""
       },
       "index" : {
         "title" : "Elasticsearch Index",
         "description" : "Specifies the name of the Elasticsearch index to be used for OpenAM audit
logging.",
         "propertyOrder" : 5400,
         "required" : true,
         "type" : "string",
         "exampleValue" : ""
       }
     }
   },
   "elasticsearchAuthentication" : {
     "type" : "object",
     "title" : "Authentication",
     "propertyOrder" : 3,
     "properties" : {
       "password" : {
         "title" : "Password",
         "description" : "Specifies the password to access the Elasticsearch server.<p><p>Required if
Elasticsearch Shield authentication is configured.",
         "propertyOrder" : 5600,
         "required" : true,
         "type" : "string",
         "format" : "password",
         "exampleValue" : ""
       },
       "username" : {
         "title" : "Username",
         "description" : "Specifies the username to access the Elasticsearch server.<p><p>Required if
Elasticsearch Shield authentication is configured.",
         "propertyOrder" : 5500,
         "required" : true,
```

```
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "commonHandler" : {
      "type" : "object",
      "title" : "General Handler Configuration",
      "propertyOrder" : 0,
      "properties" : {
        "enabled" : {
          "title" : "Enabled",
          "description" : "Enables or disables an audit event handler.",
          "propertyOrder" : 4900,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "topics" : {
          "title" : "Topics",
          "description" : "List of topics handled by an audit event handler.",
          "propertyOrder" : 5000,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        }
      }
    },
    "commonHandlerPlugin" : {
      "type" : "object",
      "title" : "Audit Event Handler Factory",
      "propertyOrder" : 1,
      "properties" : {
        "handlerFactory" : {
          "title" : "Factory Class Name",
          "description" : "The fully qualified class name of the factory
 responsible for creating the Audit Event Handler. The class must implement
 <code>org.forgerock.openam.audit.AuditEventHandlerFactory</code>.",
          "propertyOrder" : 6100,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    }
  }
}
```

delete

Usage:

```
am> delete ElasticSearch --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action ElasticSearch --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action ElasticSearch --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action ElasticSearch --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query ElasticSearch --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read ElasticSearch --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update ElasticSearch --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "elasticsearchBuffering" : {
      "type" : "object",
      "title" : "Buffering",
      "propertyOrder" : 4,
      "properties" : {
        "bufferingEnabled" : {
          "title" : "Buffering Enabled",
          "description" : "",
          "propertyOrder" : 5700,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "maxEvents" : {
          "title" : "Queue Capacity",
          "description" : "Maximum number of audit logs in the batch queue. Additional audit events
 are dropped.",
          "propertyOrder" : 5900,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "writeInterval" : {
          "title" : "Write interval (in milliseconds)",
          "description" : "Specifies the interval in milliseconds at which buffered events are written
 to Elasticsearch.",
          "propertyOrder" : 6000,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
```

```
        "batchSize" : {
          "title" : "Batch Size",
          "description" : "Maximum number of events that can be buffered (default: 10000)",
          "propertyOrder" : 5800,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        }
      }
    },
    "elasticsearchConfig" : {
      "type" : "object",
      "title" : "Elasticsearch Configuration",
      "propertyOrder" : 2,
      "properties" : {
        "host" : {
          "title" : "Server Hostname",
          "description" : "Host name or IP address of the Elasticsearch server.",
          "propertyOrder" : 5100,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "sslEnabled" : {
          "title" : "SSL Enabled",
          "description" : "Specifies whether SSL is configured on the Elasticsearch server.<p><p>If
SSL is enabled, be sure to import the CA certificate used to sign Elasticsearch node certificates
into the Java keystore on the host that runs OpenAM before attempting to log audit events to
Elasticsearch.",
          "propertyOrder" : 5300,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "port" : {
          "title" : "Server Port",
          "description" : "Specifies the port number used to access Elasticsearch's REST API.",
          "propertyOrder" : 5200,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "index" : {
          "title" : "Elasticsearch Index",
          "description" : "Specifies the name of the Elasticsearch index to be used for OpenAM audit
logging.",
          "propertyOrder" : 5400,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "elasticsearchAuthentication" : {
      "type" : "object",
      "title" : "Authentication",
      "propertyOrder" : 3,
      "properties" : {
        "password" : {
```

```
          "title" : "Password",
          "description" : "Specifies the password to access the Elasticsearch server.<p><p>Required if
Elasticsearch Shield authentication is configured.",
          "propertyOrder" : 5600,
          "required" : true,
          "type" : "string",
          "format" : "password",
          "exampleValue" : ""
        },
        "username" : {
          "title" : "Username",
          "description" : "Specifies the username to access the Elasticsearch server.<p><p>Required if
Elasticsearch Shield authentication is configured.",
          "propertyOrder" : 5500,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "commonHandler" : {
      "type" : "object",
      "title" : "General Handler Configuration",
      "propertyOrder" : 0,
      "properties" : {
        "enabled" : {
          "title" : "Enabled",
          "description" : "Enables or disables an audit event handler.",
          "propertyOrder" : 4900,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "topics" : {
          "title" : "Topics",
          "description" : "List of topics handled by an audit event handler.",
          "propertyOrder" : 5000,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        }
      }
    },
    "commonHandlerPlugin" : {
      "type" : "object",
      "title" : "Audit Event Handler Factory",
      "propertyOrder" : 1,
      "properties" : {
        "handlerFactory" : {
          "title" : "Factory Class Name",
          "description" : "The fully qualified class name of the factory
responsible for creating the Audit Event Handler. The class must implement
<code>org.forgerock.openam.audit.AuditEventHandlerFactory</code>.",
          "propertyOrder" : 6100,
          "required" : true,
          "type" : "string",
```

```
          "exampleValue" : ""
        }
      }
    }
  }
}
```

Global Operations

Resource path: `/global-config/services/audit/Elasticsearch`

Resource version: `1.0`

create

Usage:

```
am> create ElasticSearch --global --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "elasticsearchBuffering" : {
      "type" : "object",
      "title" : "Buffering",
      "propertyOrder" : 4,
      "properties" : {
        "bufferingEnabled" : {
          "title" : "Buffering Enabled",
          "description" : "",
          "propertyOrder" : 5700,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "maxEvents" : {
          "title" : "Queue Capacity",
          "description" : "Maximum number of audit logs in the batch queue. Additional audit events
 are dropped.",
          "propertyOrder" : 5900,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
```

```
       "batchSize" : {
         "title" : "Batch Size",
         "description" : "Maximum number of events that can be buffered (default: 10000)",
         "propertyOrder" : 5800,
         "required" : true,
         "type" : "integer",
         "exampleValue" : ""
       },
       "writeInterval" : {
         "title" : "Write interval (in milliseconds)",
         "description" : "Specifies the interval in milliseconds at which buffered events are written
to Elasticsearch.",
         "propertyOrder" : 6000,
         "required" : true,
         "type" : "integer",
         "exampleValue" : ""
       }
     }
   },
   "commonHandler" : {
     "type" : "object",
     "title" : "General Handler Configuration",
     "propertyOrder" : 0,
     "properties" : {
       "enabled" : {
         "title" : "Enabled",
         "description" : "Enables or disables an audit event handler.",
         "propertyOrder" : 4900,
         "required" : true,
         "type" : "boolean",
         "exampleValue" : ""
       },
       "topics" : {
         "title" : "Topics",
         "description" : "List of topics handled by an audit event handler.",
         "propertyOrder" : 5000,
         "required" : true,
         "items" : {
           "type" : "string"
         },
         "type" : "array",
         "exampleValue" : ""
       }
     }
   },
   "commonHandlerPlugin" : {
     "type" : "object",
     "title" : "Audit Event Handler Factory",
     "propertyOrder" : 1,
     "properties" : {
       "handlerFactory" : {
         "title" : "Factory Class Name",
         "description" : "The fully qualified class name of the factory
responsible for creating the Audit Event Handler. The class must implement
<code>org.forgerock.openam.audit.AuditEventHandlerFactory</code>.",
         "propertyOrder" : 6100,
         "required" : true,
         "type" : "string",
         "exampleValue" : ""
```

```
      }
    }
  },
  "elasticsearchConfig" : {
    "type" : "object",
    "title" : "Elasticsearch Configuration",
    "propertyOrder" : 2,
    "properties" : {
      "port" : {
        "title" : "Server Port",
        "description" : "Specifies the port number used to access Elasticsearch's REST API.",
        "propertyOrder" : 5200,
        "required" : true,
        "type" : "integer",
        "exampleValue" : ""
      },
      "sslEnabled" : {
        "title" : "SSL Enabled",
        "description" : "Specifies whether SSL is configured on the Elasticsearch server.<p><p>If
SSL is enabled, be sure to import the CA certificate used to sign Elasticsearch node certificates
into the Java keystore on the host that runs OpenAM before attempting to log audit events to
Elasticsearch.",
        "propertyOrder" : 5300,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
      },
      "host" : {
        "title" : "Server Hostname",
        "description" : "Host name or IP address of the Elasticsearch server.",
        "propertyOrder" : 5100,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
      },
      "index" : {
        "title" : "Elasticsearch Index",
        "description" : "Specifies the name of the Elasticsearch index to be used for OpenAM audit
logging.",
        "propertyOrder" : 5400,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
      }
    }
  },
  "elasticsearchAuthentication" : {
    "type" : "object",
    "title" : "Authentication",
    "propertyOrder" : 3,
    "properties" : {
      "username" : {
        "title" : "Username",
        "description" : "Specifies the username to access the Elasticsearch server.<p><p>Required if
Elasticsearch Shield authentication is configured.",
        "propertyOrder" : 5500,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
```

```
        },
        "password" : {
          "title" : "Password",
          "description" : "Specifies the password to access the Elasticsearch server.<p><p>Required if
 Elasticsearch Shield authentication is configured.",
          "propertyOrder" : 5600,
          "required" : true,
          "type" : "string",
          "format" : "password",
          "exampleValue" : ""
        }
      }
    }
  }
}
```

delete

Usage:

```
am> delete ElasticSearch --global --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action ElasticSearch --global --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action ElasticSearch --global --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action ElasticSearch --global --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query ElasticSearch --global --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read ElasticSearch --global --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update ElasticSearch --global --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "elasticsearchBuffering" : {
      "type" : "object",
      "title" : "Buffering",
      "propertyOrder" : 4,
      "properties" : {
        "bufferingEnabled" : {
          "title" : "Buffering Enabled",
          "description" : "",
          "propertyOrder" : 5700,
```

```
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "maxEvents" : {
          "title" : "Queue Capacity",
          "description" : "Maximum number of audit logs in the batch queue. Additional audit events
are dropped.",
          "propertyOrder" : 5900,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "batchSize" : {
          "title" : "Batch Size",
          "description" : "Maximum number of events that can be buffered (default: 10000)",
          "propertyOrder" : 5800,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "writeInterval" : {
          "title" : "Write interval (in milliseconds)",
          "description" : "Specifies the interval in milliseconds at which buffered events are written
to Elasticsearch.",
          "propertyOrder" : 6000,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        }
      }
    },
    "commonHandler" : {
      "type" : "object",
      "title" : "General Handler Configuration",
      "propertyOrder" : 0,
      "properties" : {
        "enabled" : {
          "title" : "Enabled",
          "description" : "Enables or disables an audit event handler.",
          "propertyOrder" : 4900,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "topics" : {
          "title" : "Topics",
          "description" : "List of topics handled by an audit event handler.",
          "propertyOrder" : 5000,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        }
      }
    },
    "commonHandlerPlugin" : {
```

```
      "type" : "object",
      "title" : "Audit Event Handler Factory",
      "propertyOrder" : 1,
      "properties" : {
        "handlerFactory" : {
          "title" : "Factory Class Name",
          "description" : "The fully qualified class name of the factory
responsible for creating the Audit Event Handler. The class must implement
<code>org.forgerock.openam.audit.AuditEventHandlerFactory</code>.",
          "propertyOrder" : 6100,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "elasticsearchConfig" : {
      "type" : "object",
      "title" : "Elasticsearch Configuration",
      "propertyOrder" : 2,
      "properties" : {
        "port" : {
          "title" : "Server Port",
          "description" : "Specifies the port number used to access Elasticsearch's REST API.",
          "propertyOrder" : 5200,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "sslEnabled" : {
          "title" : "SSL Enabled",
          "description" : "Specifies whether SSL is configured on the Elasticsearch server.<p><p>If
SSL is enabled, be sure to import the CA certificate used to sign Elasticsearch node certificates
into the Java keystore on the host that runs OpenAM before attempting to log audit events to
Elasticsearch.",
          "propertyOrder" : 5300,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "host" : {
          "title" : "Server Hostname",
          "description" : "Host name or IP address of the Elasticsearch server.",
          "propertyOrder" : 5100,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "index" : {
          "title" : "Elasticsearch Index",
          "description" : "Specifies the name of the Elasticsearch index to be used for OpenAM audit
logging.",
          "propertyOrder" : 5400,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
```

```
    "elasticsearchAuthentication" : {
      "type" : "object",
      "title" : "Authentication",
      "propertyOrder" : 3,
      "properties" : {
        "username" : {
          "title" : "Username",
          "description" : "Specifies the username to access the Elasticsearch server.<p><p>Required if
 Elasticsearch Shield authentication is configured.",
          "propertyOrder" : 5500,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "password" : {
          "title" : "Password",
          "description" : "Specifies the password to access the Elasticsearch server.<p><p>Required if
 Elasticsearch Shield authentication is configured.",
          "propertyOrder" : 5600,
          "required" : true,
          "type" : "string",
          "format" : "password",
          "exampleValue" : ""
        }
      }
    }
  }
}
```

EmailService

Realm Operations

Resource path: `/realm-config/services/email`

Resource version: `1.0`

create

Usage:

```
am> create EmailService --realm Realm --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
```

```
 "properties" : {
   "sslState" : {
     "title" : "Mail Server Secure Connection",
     "description" : "Specifies whether to connect to the SMTP mail server using SSL.",
     "propertyOrder" : 600,
     "required" : true,
     "type" : "string",
     "exampleValue" : ""
   },
   "subject" : {
     "title" : "Email Subject",
     "description" : "Specifies a subject for notification messages. If you do not set this, OpenAM
does not set the subject for notification messages.",
     "propertyOrder" : 900,
     "required" : false,
     "type" : "string",
     "exampleValue" : ""
   },
   "emailAddressAttribute" : {
     "title" : "Email Attribute Name",
     "description" : "Specifies the profile attribute from which to retrieve the end user's email
address.",
     "propertyOrder" : 800,
     "required" : true,
     "type" : "string",
     "exampleValue" : ""
   },
   "emailRateLimitSeconds" : {
     "title" : "Email Rate Limit",
     "description" : "Specifies the minimum number of seconds which must elapse between sending
emails to an individual user.",
     "propertyOrder" : 1100,
     "required" : true,
     "type" : "integer",
     "exampleValue" : ""
   },
   "hostname" : {
     "title" : "Mail Server Host Name",
     "description" : "Specifies the fully qualified domain name of the SMTP mail server through which
to send email notifications.",
     "propertyOrder" : 200,
     "required" : true,
     "type" : "string",
     "exampleValue" : "smtp.example.com"
   },
   "from" : {
     "title" : "Email From Address",
     "description" : "Specifies the address from which to send email notifications.",
     "propertyOrder" : 700,
     "required" : true,
     "type" : "string",
     "exampleValue" : "no-reply@example.com"
   },
   "message" : {
     "title" : "Email Content",
     "description" : "Specifies content for notification messages. If you do not set this, OpenAM
includes only the confirmation URL in the mail body.",
     "propertyOrder" : 1000,
     "required" : false,
```

```
      "type" : "string",
      "exampleValue" : ""
    },
    "password" : {
      "title" : "Mail Server Authentication Password",
      "description" : "Specifies the password for the SMTP user name.",
      "propertyOrder" : 500,
      "required" : true,
      "type" : "string",
      "format" : "password",
      "exampleValue" : ""
    },
    "port" : {
      "title" : "Mail Server Host Port",
      "description" : "Specifies the port number for the SMTP mail server.",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "username" : {
      "title" : "Mail Server Authentication Username",
      "description" : "Specifies the user name for the SMTP mail server.",
      "propertyOrder" : 400,
      "required" : true,
      "type" : "string",
      "exampleValue" : "username"
    },
    "emailImplClassName" : {
      "title" : "Email Message Implementation Class",
      "description" : "Specifies the class that sends email notifications, such as those sent for user
 registration and forgotten passwords.",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
```

delete

Usage:

```
am> delete EmailService --realm Realm
```

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action EmailService --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action EmailService --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action EmailService --realm Realm --actionName nextdescendents
```

read

Usage:

```
am> read EmailService --realm Realm
```

update

Usage:

```
am> update EmailService --realm Realm --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "sslState" : {
      "title" : "Mail Server Secure Connection",
      "description" : "Specifies whether to connect to the SMTP mail server using SSL.",
      "propertyOrder" : 600,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "subject" : {
      "title" : "Email Subject",
      "description" : "Specifies a subject for notification messages. If you do not set this, OpenAM
 does not set the subject for notification messages.",
      "propertyOrder" : 900,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
```

```
   },
   "emailAddressAttribute" : {
     "title" : "Email Attribute Name",
     "description" : "Specifies the profile attribute from which to retrieve the end user's email
address.",
     "propertyOrder" : 800,
     "required" : true,
     "type" : "string",
     "exampleValue" : ""
   },
   "emailRateLimitSeconds" : {
     "title" : "Email Rate Limit",
     "description" : "Specifies the minimum number of seconds which must elapse between sending
emails to an individual user.",
     "propertyOrder" : 1100,
     "required" : true,
     "type" : "integer",
     "exampleValue" : ""
   },
   "hostname" : {
     "title" : "Mail Server Host Name",
     "description" : "Specifies the fully qualified domain name of the SMTP mail server through which
to send email notifications.",
     "propertyOrder" : 200,
     "required" : true,
     "type" : "string",
     "exampleValue" : "smtp.example.com"
   },
   "from" : {
     "title" : "Email From Address",
     "description" : "Specifies the address from which to send email notifications.",
     "propertyOrder" : 700,
     "required" : true,
     "type" : "string",
     "exampleValue" : "no-reply@example.com"
   },
   "message" : {
     "title" : "Email Content",
     "description" : "Specifies content for notification messages. If you do not set this, OpenAM
includes only the confirmation URL in the mail body.",
     "propertyOrder" : 1000,
     "required" : false,
     "type" : "string",
     "exampleValue" : ""
   },
   "password" : {
     "title" : "Mail Server Authentication Password",
     "description" : "Specifies the password for the SMTP user name.",
     "propertyOrder" : 500,
     "required" : true,
     "type" : "string",
     "format" : "password",
     "exampleValue" : ""
   },
   "port" : {
     "title" : "Mail Server Host Port",
     "description" : "Specifies the port number for the SMTP mail server.",
     "propertyOrder" : 300,
     "required" : true,
```

```
      "type" : "integer",
      "exampleValue" : ""
    },
    "username" : {
      "title" : "Mail Server Authentication Username",
      "description" : "Specifies the user name for the SMTP mail server.",
      "propertyOrder" : 400,
      "required" : true,
      "type" : "string",
      "exampleValue" : "username"
    },
    "emailImplClassName" : {
      "title" : "Email Message Implementation Class",
      "description" : "Specifies the class that sends email notifications, such as those sent for user
 registration and forgotten passwords.",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
```

Global Operations

Resource path: `/global-config/services/email`

Resource version: `1.0`

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action EmailService --global --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action EmailService --global --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action EmailService --global --actionName nextdescendents
```

read

Usage:

```
am> read EmailService --global
```

update

Usage:

```
am> update EmailService --global --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "defaults" : {
      "properties" : {
        "password" : {
          "title" : "Mail Server Authentication Password",
          "description" : "Specifies the password for the SMTP user name.",
          "propertyOrder" : 500,
          "required" : true,
          "type" : "string",
          "format" : "password",
          "exampleValue" : ""
        },
        "port" : {
          "title" : "Mail Server Host Port",
          "description" : "Specifies the port number for the SMTP mail server.",
          "propertyOrder" : 300,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "sslState" : {
          "title" : "Mail Server Secure Connection",
          "description" : "Specifies whether to connect to the SMTP mail server using SSL.",
          "propertyOrder" : 600,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "subject" : {
          "title" : "Email Subject",
          "description" : "Specifies a subject for notification messages. If you do not set this,
 OpenAM does not set the subject for notification messages.",
          "propertyOrder" : 900,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
```

```
      },
      "message" : {
        "title" : "Email Content",
        "description" : "Specifies content for notification messages. If you do not set this, OpenAM
includes only the confirmation URL in the mail body.",
        "propertyOrder" : 1000,
        "required" : false,
        "type" : "string",
        "exampleValue" : ""
      },
      "hostname" : {
        "title" : "Mail Server Host Name",
        "description" : "Specifies the fully qualified domain name of the SMTP mail server through
which to send email notifications.",
        "propertyOrder" : 200,
        "required" : true,
        "type" : "string",
        "exampleValue" : "smtp.example.com"
      },
      "emailRateLimitSeconds" : {
        "title" : "Email Rate Limit",
        "description" : "Specifies the minimum number of seconds which must elapse between sending
emails to an individual user.",
        "propertyOrder" : 1100,
        "required" : true,
        "type" : "integer",
        "exampleValue" : ""
      },
      "emailImplClassName" : {
        "title" : "Email Message Implementation Class",
        "description" : "Specifies the class that sends email notifications, such as those sent for
user registration and forgotten passwords.",
        "propertyOrder" : 100,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
      },
      "username" : {
        "title" : "Mail Server Authentication Username",
        "description" : "Specifies the user name for the SMTP mail server.",
        "propertyOrder" : 400,
        "required" : true,
        "type" : "string",
        "exampleValue" : "username"
      },
      "from" : {
        "title" : "Email From Address",
        "description" : "Specifies the address from which to send email notifications.",
        "propertyOrder" : 700,
        "required" : true,
        "type" : "string",
        "exampleValue" : "no-reply@example.com"
      },
      "emailAddressAttribute" : {
        "title" : "Email Attribute Name",
        "description" : "Specifies the profile attribute from which to retrieve the end user's email
address.",
        "propertyOrder" : 800,
        "required" : true,
```

```
          "type" : "string",
          "exampleValue" : ""
        }
      },
      "type" : "object",
      "title" : "Realm Defaults"
    }
  }
}
```

EmailSuspendNode

Realm Operations

Resource path: `/realm-config/authentication/authenticationtrees/nodes/EmailSuspendNode`

Resource version: `1.0`

create

Usage:

```
am> create EmailSuspendNode --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "objectLookup" : {
      "title" : "Object Lookup",
      "description" : "Determines whether object lookup should occur. If true, existing object is
 queried. Otherwise, object in shared state is used for template object.",
      "propertyOrder" : 400,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "emailTemplateName" : {
      "title" : "Email Template Name",
      "description" : "The IDM email template to be sent.",
      "propertyOrder" : 100,
```

```
      "type" : "string",
      "exampleValue" : ""
    },
    "emailAttribute" : {
      "title" : "Email Attribute",
      "description" : "The IDM email field to send the email to.",
      "propertyOrder" : 200,
      "type" : "string",
      "exampleValue" : ""
    },
    "identityAttribute" : {
      "title" : "Identity Attribute",
      "description" : "The attribute used to identify the the object in IDM.",
      "propertyOrder" : 500,
      "type" : "string",
      "exampleValue" : ""
    },
    "emailSuspendMessage" : {
      "title" : "Email Suspend Message",
      "description" : "The localised message to be returned once the tree is suspended.",
      "propertyOrder" : 300,
      "patternProperties" : {
        ".*" : {
          "type" : "string"
        }
      },
      "type" : "object",
      "exampleValue" : ""
    }
  },
  "required" : [ "emailSuspendMessage", "emailTemplateName", "objectLookup", "identityAttribute",
 "emailAttribute" ]
}
```

delete

Usage:

```
am> delete EmailSuspendNode --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action EmailSuspendNode --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action EmailSuspendNode --realm Realm --actionName getCreatableTypes
```

listOutcomes

List the available outcomes for the node type.

Usage:

```
am> action EmailSuspendNode --realm Realm --body body --actionName listOutcomes
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "title" : "Some configuration of the node. This does not need to be complete against the
 configuration schema."
}
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action EmailSuspendNode --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query EmailSuspendNode --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read EmailSuspendNode --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update EmailSuspendNode --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "objectLookup" : {
      "title" : "Object Lookup",
      "description" : "Determines whether object lookup should occur. If true, existing object is
 queried. Otherwise, object in shared state is used for template object.",
      "propertyOrder" : 400,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "emailTemplateName" : {
      "title" : "Email Template Name",
      "description" : "The IDM email template to be sent.",
      "propertyOrder" : 100,
      "type" : "string",
      "exampleValue" : ""
    },
    "emailAttribute" : {
      "title" : "Email Attribute",
      "description" : "The IDM email field to send the email to.",
      "propertyOrder" : 200,
      "type" : "string",
      "exampleValue" : ""
```

```
    },
    "identityAttribute" : {
      "title" : "Identity Attribute",
      "description" : "The attribute used to identify the the object in IDM.",
      "propertyOrder" : 500,
      "type" : "string",
      "exampleValue" : ""
    },
    "emailSuspendMessage" : {
      "title" : "Email Suspend Message",
      "description" : "The localised message to be returned once the tree is suspended.",
      "propertyOrder" : 300,
      "patternProperties" : {
        ".*" : {
          "type" : "string"
        }
      },
      "type" : "object",
      "exampleValue" : ""
    }
  },
  "required" : [ "emailSuspendMessage", "emailTemplateName", "objectLookup", "identityAttribute",
 "emailAttribute" ]
}
```

EmailTemplateNode

Realm Operations

Resource path: `/realm-config/authentication/authenticationtrees/nodes/EmailTemplateNode`

Resource version: `1.0`

create

Usage:

```
am> create EmailTemplateNode --realm Realm --id id --body body
```

Parameters:

`--id`

The unique identifier for the resource.

`--body`

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "emailAttribute" : {
      "title" : "Email Attribute",
      "description" : "The IDM email field to send the email to.",
      "propertyOrder" : 200,
      "type" : "string",
      "exampleValue" : ""
    },
    "identityAttribute" : {
      "title" : "Identity Attribute",
      "description" : "The attribute used to identify the the object in IDM.",
      "propertyOrder" : 300,
      "type" : "string",
      "exampleValue" : ""
    },
    "emailTemplateName" : {
      "title" : "Email Template Name",
      "description" : "The IDM email template to be sent.",
      "propertyOrder" : 100,
      "type" : "string",
      "exampleValue" : ""
    }
  },
  "required" : [ "identityAttribute", "emailAttribute", "emailTemplateName" ]
}
```

delete

Usage:

```
am> delete EmailTemplateNode --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action EmailTemplateNode --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action EmailTemplateNode --realm Realm --actionName getCreatableTypes
```

listOutcomes

List the available outcomes for the node type.

Usage:

```
am> action EmailTemplateNode --realm Realm --body body --actionName listOutcomes
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "title" : "Some configuration of the node. This does not need to be complete against the
 configuration schema."
}
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action EmailTemplateNode --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query EmailTemplateNode --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read EmailTemplateNode --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update EmailTemplateNode --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "emailAttribute" : {
      "title" : "Email Attribute",
      "description" : "The IDM email field to send the email to.",
      "propertyOrder" : 200,
      "type" : "string",
      "exampleValue" : ""
    },
    "identityAttribute" : {
      "title" : "Identity Attribute",
      "description" : "The attribute used to identify the the object in IDM.",
      "propertyOrder" : 300,
      "type" : "string",
      "exampleValue" : ""
    },
    "emailTemplateName" : {
      "title" : "Email Template Name",
      "description" : "The IDM email template to be sent.",
      "propertyOrder" : 100,
      "type" : "string",
      "exampleValue" : ""
    }
  },
  "required" : [ "identityAttribute", "emailAttribute", "emailTemplateName" ]
}
```

EnvironmentAndSystemPropertySecretsStore

Global Operations

Resource path: `/global-config/secrets/stores/EnvironmentAndSystemPropertySecretStore`

Resource version: `1.0`

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action EnvironmentAndSystemPropertySecretsStore --global --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action EnvironmentAndSystemPropertySecretsStore --global --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action EnvironmentAndSystemPropertySecretsStore --global --actionName nextdescendents
```

read

Usage:

```
am> read EnvironmentAndSystemPropertySecretsStore --global
```

update

Usage:

```
am> update EnvironmentAndSystemPropertySecretsStore --global --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "format" : {
      "title" : "Value format",
      "description" : "Indicates the format used to store the secrets. The available options are: <ul>
 <li>Plain text: the secrets are stored as UTF-8 encoded text.</li> <li>Base64 encoded: the secrets
 are stored as Base64 encoded binary values.</li> <li>Encrypted text: the plain text secrets are
 encrypted using AM's encryption key.</li> <li>Encrypted Base64 encoded: the Base64 encoded binary
 values are encrypted using AM's encryption key.</li>  <li>Encrypted HMAC key: the Base64 encoded
 binary representation of the HMAC key is encrypted using AM's encryption key. Use this format when
 working with non generic secrets.</li> <li>Base64 encoded HMAC key: the secrets are binary HMAC keys
 encoded with Base64.</li> <li>Encrypted with Google KMS: the secrets are encrypted using Google's
 Key Management Service.</li> <li>Google KMS-encrypted HMAC key: the secrets are binary HMAC keys that
 have been encrypted with Google's Key Management Service (KMS).</li> </ul>",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
```

FailureURL

Realm Operations

Resource path: `/realm-config/authentication/authenticationtrees/nodes/SetFailureUrlNode`

Resource version: `1.0`

create

Usage:

```
am> create FailureURL --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "failureUrl" : {
      "title" : "Failure URL",
      "description" : "",
      "propertyOrder" : 100,
      "type" : "string",
      "exampleValue" : ""
    }
  },
  "required" : [ "failureUrl" ]
}
```

delete

Usage:

```
am> delete FailureURL --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action FailureURL --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action FailureURL --realm Realm --actionName getCreatableTypes
```

listOutcomes

List the available outcomes for the node type.

Usage:

```
am> action FailureURL --realm Realm --body body --actionName listOutcomes
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "title" : "Some configuration of the node. This does not need to be complete against the
 configuration schema."
}
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action FailureURL --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query FailureURL --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read FailureURL --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update FailureURL --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "failureUrl" : {
      "title" : "Failure URL",
      "description" : "",
      "propertyOrder" : 100,
      "type" : "string",
      "exampleValue" : ""
    }
  },
  "required" : [ "failureUrl" ]
}
```

FederationModule

Realm Operations

Resource path: `/realm-config/authentication/modules/federation`

Resource version: `1.0`

create

Usage:

```
am> create FederationModule --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "authenticationLevel" : {
      "title" : "Authentication Level",
      "description" : "The authentication level associated with this module.<br><br>Each
 authentication module has an authentication level that can be used to indicate the level of security
 associated with the module; 0 is the lowest (and the default).",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    }
  }
}
```

delete

Usage:

```
am> delete FederationModule --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action FederationModule --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action FederationModule --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action FederationModule --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query FederationModule --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read FederationModule --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update FederationModule --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "authenticationLevel" : {
      "title" : "Authentication Level",
      "description" : "The authentication level associated with this module.<br><br>Each
 authentication module has an authentication level that can be used to indicate the level of security
 associated with the module; 0 is the lowest (and the default).",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    }
  }
}
```

Global Operations

Resource path: `/global-config/authentication/modules/federation`

Resource version: `1.0`

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action FederationModule --global --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action FederationModule --global --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action FederationModule --global --actionName nextdescendents
```

read

Usage:

```
am> read FederationModule --global
```

update

Usage:

```
am> update FederationModule --global --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "defaults" : {
      "properties" : {
        "authenticationLevel" : {
          "title" : "Authentication Level",
          "description" : "The authentication level associated with this module.<br><br>Each
 authentication module has an authentication level that can be used to indicate the level of security
 associated with the module; 0 is the lowest (and the default).",
          "propertyOrder" : 100,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        }
      },
      "type" : "object",
      "title" : "Realm Defaults"
    }
  }
}
```

FileSystemSecretStore

Realm Operations

Resource path: `/realm-config/secrets/stores/FileSystemSecretStore`

Resource version: `1.0`

create

Usage:

```
am> create FileSystemSecretStore --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "directory" : {
      "title" : "Directory",
      "description" : "The directory containing secret files.",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "suffix" : {
      "title" : "File suffix",
      "description" : "A suffix to add to the name of each secret to obtain the file name, such as
 \".txt\" (defaults to no suffix).",
      "propertyOrder" : 200,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
    },
    "format" : {
      "title" : "File format",
      "description" : "Indicates what format is used to store the secrets in the files. The available
 options are: <ul> <li>Plain text: the secrets are stored as UTF-8 encoded text.</li> <li>Base64
 encoded: the secrets are stored as Base64 encoded binary values.</li> <li>Encrypted text: the plain
 text secrets are encrypted using AM's encryption key.</li> <li>Encrypted Base64 encoded: the Base64
 encoded binary values are encrypted using AM's encryption key.</li>  <li>Encrypted HMAC key: the
 Base64 encoded binary representation of the HMAC key is encrypted using AM's encryption key. Use
 this format when working with non generic secrets.</li> <li>Base64 encoded HMAC key: the secrets are
 binary HMAC keys encoded with Base64.</li> <li>Encrypted with Google KMS: the secrets are encrypted
 using Google's Key Management Service.</li> <li>Google KMS-encrypted HMAC key: the secrets are binary
 HMAC keys that have been encrypted with Google's Key Management Service (KMS).</li> </ul>",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
```

delete

Usage:

```
am> delete FileSystemSecretStore --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action FileSystemSecretStore --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action FileSystemSecretStore --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action FileSystemSecretStore --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query FileSystemSecretStore --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read FileSystemSecretStore --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update FileSystemSecretStore --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "directory" : {
      "title" : "Directory",
      "description" : "The directory containing secret files.",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "suffix" : {
      "title" : "File suffix",
      "description" : "A suffix to add to the name of each secret to obtain the file name, such as
 \".txt\" (defaults to no suffix).",
      "propertyOrder" : 200,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
    },
    "format" : {
      "title" : "File format",
      "description" : "Indicates what format is used to store the secrets in the files. The available
 options are: <ul> <li>Plain text: the secrets are stored as UTF-8 encoded text.</li> <li>Base64
 encoded: the secrets are stored as Base64 encoded binary values.</li> <li>Encrypted text: the plain
 text secrets are encrypted using AM's encryption key.</li> <li>Encrypted Base64 encoded: the Base64
 encoded binary values are encrypted using AM's encryption key.</li>  <li>Encrypted HMAC key: the
 Base64 encoded binary representation of the HMAC key is encrypted using AM's encryption key. Use
 this format when working with non generic secrets.</li> <li>Base64 encoded HMAC key: the secrets are
 binary HMAC keys encoded with Base64.</li> <li>Encrypted with Google KMS: the secrets are encrypted
 using Google's Key Management Service.</li> <li>Google KMS-encrypted HMAC key: the secrets are binary
 HMAC keys that have been encrypted with Google's Key Management Service (KMS).</li> </ul>",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
```

Global Operations

Resource path: `/global-config/secrets/stores/FileSystemSecretStore`

Resource version: `1.0`

create

Usage:

```
am> create FileSystemSecretStore --global --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "directory" : {
      "title" : "Directory",
      "description" : "The directory containing secret files.",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "suffix" : {
      "title" : "File suffix",
      "description" : "A suffix to add to the name of each secret to obtain the file name, such as
 \".txt\" (defaults to no suffix).",
      "propertyOrder" : 200,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
    },
    "format" : {
      "title" : "File format",
      "description" : "Indicates what format is used to store the secrets in the files. The available
 options are: <ul> <li>Plain text: the secrets are stored as UTF-8 encoded text.</li> <li>Base64
 encoded: the secrets are stored as Base64 encoded binary values.</li> <li>Encrypted text: the plain
 text secrets are encrypted using AM's encryption key.</li> <li>Encrypted Base64 encoded: the Base64
 encoded binary values are encrypted using AM's encryption key.</li>  <li>Encrypted HMAC key: the
 Base64 encoded binary representation of the HMAC key is encrypted using AM's encryption key. Use
 this format when working with non generic secrets.</li> <li>Base64 encoded HMAC key: the secrets are
 binary HMAC keys encoded with Base64.</li> <li>Encrypted with Google KMS: the secrets are encrypted
 using Google's Key Management Service.</li> <li>Google KMS-encrypted HMAC key: the secrets are binary
 HMAC keys that have been encrypted with Google's Key Management Service (KMS).</li> </ul>",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
```

delete

Usage:

```
am> delete FileSystemSecretStore --global --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action FileSystemSecretStore --global --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action FileSystemSecretStore --global --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action FileSystemSecretStore --global --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query FileSystemSecretStore --global --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read FileSystemSecretStore --global --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update FileSystemSecretStore --global --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "directory" : {
      "title" : "Directory",
      "description" : "The directory containing secret files.",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "suffix" : {
      "title" : "File suffix",
      "description" : "A suffix to add to the name of each secret to obtain the file name, such as
 \".txt\" (defaults to no suffix).",
      "propertyOrder" : 200,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
    },
    "format" : {
      "title" : "File format",
      "description" : "Indicates what format is used to store the secrets in the files. The available
 options are: <ul> <li>Plain text: the secrets are stored as UTF-8 encoded text.</li> <li>Base64
 encoded: the secrets are stored as Base64 encoded binary values.</li> <li>Encrypted text: the plain
 text secrets are encrypted using AM's encryption key.</li> <li>Encrypted Base64 encoded: the Base64
 encoded binary values are encrypted using AM's encryption key.</li>  <li>Encrypted HMAC key: the
 Base64 encoded binary representation of the HMAC key is encrypted using AM's encryption key. Use
 this format when working with non generic secrets.</li> <li>Base64 encoded HMAC key: the secrets are
 binary HMAC keys encoded with Base64.</li> <li>Encrypted with Google KMS: the secrets are encrypted
 using Google's Key Management Service.</li> <li>Google KMS-encrypted HMAC key: the secrets are binary
 HMAC keys that have been encrypted with Google's Key Management Service (KMS).</li> </ul>",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
```


ForgeRockIAMDirectoryServer

Realm Operations

Resource path: `/realm-config/services/id-repositories/LDAPv3ForForgeRockIAM`

Resource version: `1.0`

create

Usage:

```
am> create ForgeRockIAMDirectoryServer --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "userconfig" : {
      "type" : "object",
      "title" : "User Configuration",
      "propertyOrder" : 3,
      "properties" : {
        "sun-idrepo-ldapv3-config-people-container-name" : {
          "title" : "LDAP People Container Naming Attribute",
          "description" : "",
          "propertyOrder" : 5000,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-active" : {
          "title" : "User Status Active Value",
          "description" : "",
          "propertyOrder" : 2700,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-users-search-attribute" : {
          "title" : "LDAP Users  Search Attribute",
          "description" : "",
          "propertyOrder" : 2100,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-auth-kba-index-attr" : {
          "title" : "Knowledge Based Authentication Active Index",
          "description" : "",
          "propertyOrder" : 5400,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-users-search-filter" : {
          "title" : "LDAP Users  Search Filter",
          "description" : "",
          "propertyOrder" : 2200,
          "required" : false,
```

```
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-user-objectclass" : {
          "title" : "LDAP User Object Class",
          "description" : "",
          "propertyOrder" : 2300,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-createuser-attr-mapping" : {
          "title" : "Create User Attribute Mapping",
          "description" : "Format: attribute name or TargetAttributeName=SourceAttributeName",
          "propertyOrder" : 2500,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-auth-kba-attr" : {
          "title" : "Knowledge Based Authentication Attribute Name",
          "description" : "",
          "propertyOrder" : 5300,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-people-container-value" : {
          "title" : "LDAP People Container Value",
          "description" : "",
          "propertyOrder" : 5100,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-auth-kba-attempts-attr" : {
          "title" : "Knowledge Based Authentication Attempts Attribute Name",
          "description" : "",
          "propertyOrder" : 5410,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-inactive" : {
          "title" : "User Status Inactive Value",
          "description" : "",
          "propertyOrder" : 2800,
```

```
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-user-attributes" : {
          "title" : "LDAP User Attributes",
          "description" : "",
          "propertyOrder" : 2400,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-isactive" : {
          "title" : "Attribute Name of User Status",
          "description" : "",
          "propertyOrder" : 2600,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "persistentsearch" : {
      "type" : "object",
      "title" : "Persistent Search Controls",
      "propertyOrder" : 7,
      "properties" : {
        "sun-idrepo-ldapv3-config-psearch-scope" : {
          "title" : "Persistent Search Scope",
          "description" : "",
          "propertyOrder" : 5700,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-psearch-filter" : {
          "title" : "Persistent Search Filter",
          "description" : "",
          "propertyOrder" : 5600,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-psearchbase" : {
          "title" : "Persistent Search Base DN",
          "description" : "",
          "propertyOrder" : 5500,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "ldapsettings" : {
      "type" : "object",
      "title" : "Server Settings",
```

```
     "propertyOrder" : 0,
     "properties" : {
       "openam-idrepo-ldapv3-proxied-auth-denied-fallback" : {
         "title" : "Fallback using Bind DN if Proxied Authorization denied",
         "description" : "Enable this setting to fallback and retry using non-proxied authorization
(DS proxied-auth privilege) when proxied authorization is denied. Normally this happens when the
attributes cannot be changed because the account is locked or the password has expired. This setting
is effective only when Proxied Authorization is enabled.",
         "propertyOrder" : 860,
         "required" : false,
         "type" : "boolean",
         "exampleValue" : ""
       },
       "sun-idrepo-ldapv3-config-connection-mode" : {
         "title" : "LDAP Connection Mode",
         "description" : "Defines which protocol/operation is used to establish the connection to
the LDAP Directory Server.<br><br>If 'LDAP' is selected, the connection <b>won't be secured</b> and
passwords are transferred in <b>cleartext</b> over the network.<br/> If 'LDAPS' is selected, the
connection is secured via SSL or TLS. <br/> If 'StartTLS' is selected, the connection is secured by
using StartTLS extended operation.",
         "propertyOrder" : 1000,
         "required" : false,
         "type" : "string",
         "exampleValue" : ""
       },
       "sun-idrepo-ldapv3-config-max-result" : {
         "title" : "Maximum Results Returned from Search",
         "description" : "",
         "propertyOrder" : 1500,
         "required" : false,
         "type" : "integer",
         "exampleValue" : ""
       },
       "sun-idrepo-ldapv3-config-connection_pool_max_size" : {
         "title" : "LDAP Connection Pool Maximum Size",
         "description" : "",
         "propertyOrder" : 1200,
         "required" : false,
         "type" : "integer",
         "exampleValue" : ""
       },
       "sun-idrepo-ldapv3-config-time-limit" : {
         "title" : "Search Timeout",
         "description" : "In seconds.",
         "propertyOrder" : 1600,
         "required" : false,
         "type" : "integer",
         "exampleValue" : ""
       },
       "sun-idrepo-ldapv3-config-authid" : {
         "title" : "LDAP Bind DN",
         "description" : "A user or admin with sufficient access rights to perform the supported
operations.",
         "propertyOrder" : 700,
         "required" : false,
         "type" : "string",
         "exampleValue" : ""
       },
       "sun-idrepo-ldapv3-config-connection_pool_min_size" : {
```

```
          "title" : "LDAP Connection Pool Minimum Size",
          "description" : "",
          "propertyOrder" : 1100,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "openam-idrepo-ldapv3-heartbeat-interval" : {
          "title" : "LDAP Connection Heartbeat Interval",
          "description" : "Specifies how often should OpenAM send a heartbeat request to the
directory.<br><br>This setting controls how often OpenAM <b>should</b> send a heartbeat search
request to the configured directory. If a connection becomes unresponsive (e.g. due to a network
error) then it may take up to the interval period before the problem is detected. Use along with the
Heartbeat Time Unit parameter to define the exact interval. Zero or negative value will result in
disabling heartbeat requests.",
          "propertyOrder" : 1300,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-authpw" : {
          "title" : "LDAP Bind Password",
          "description" : "",
          "propertyOrder" : 800,
          "required" : false,
          "type" : "string",
          "format" : "password",
          "exampleValue" : ""
        },
        "openam-idrepo-ldapv3-heartbeat-timeunit" : {
          "title" : "LDAP Connection Heartbeat Time Unit",
          "description" : "Defines the time unit corresponding to the Heartbeat Interval
setting.<br><br>This setting controls how often OpenAM <b>should</b> send a heartbeat search request
to the configured directory. If a connection becomes unresponsive (e.g. due to a network error) then
it may take up to the interval period before the problem is detected. Use along with the Heartbeat
Interval parameter to define the exact interval.",
          "propertyOrder" : 1400,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-search-scope" : {
          "title" : "LDAPv3 Plug-in Search Scope",
          "description" : "",
          "propertyOrder" : 2000,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "openam-idrepo-ldapv3-behera-support-enabled" : {
          "title" : "Behera Support Enabled",
          "description" : "When enabled, Behera draft control will be used in the outgoing requests
for operations that may modify password value. This will allow OpenAM to display password policy
related error messages when password policies are not met.",
          "propertyOrder" : 6100,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
```

```
       "openam-idrepo-ldapv3-affinity-enabled" : {
         "title" : "Affinity Enabled",
         "description" : "Enables affinity based request load balancing when accessing the user store
servers (based on DN). It is imperative that the connection string setting is set to the same value
for all OpenAM servers in the deployment when this feature is enabled.",
         "propertyOrder" : 6300,
         "required" : true,
         "type" : "boolean",
         "exampleValue" : ""
       },
       "sun-idrepo-ldapv3-config-ldap-server" : {
         "title" : "LDAP Server",
         "description" : "Format: LDAP server host name:port | server_ID | site_ID",
         "propertyOrder" : 600,
         "required" : true,
         "items" : {
           "type" : "string"
         },
         "minItems" : 1,
         "type" : "array",
         "exampleValue" : ""
       },
       "openam-idrepo-ldapv3-proxied-auth-enabled" : {
         "title" : "Proxied Authorization using Bind DN",
         "description" : "Enable this setting if you have configured the LDAP bind DN account for
proxied authorization (DS proxied-auth privilege). Do not enable this property if the LDAP bind DN
account does not have the proxied-auth privilege granted because the user would not be able to reset
their password. DS and AM log an error when this occurs.",
         "propertyOrder" : 850,
         "required" : false,
         "type" : "boolean",
         "exampleValue" : ""
       },
       "sun-idrepo-ldapv3-config-organization_name" : {
         "title" : "LDAP Organization DN",
         "description" : "",
         "propertyOrder" : 900,
         "required" : true,
         "type" : "string",
         "exampleValue" : ""
       }
     }
   },
   "cachecontrol" : {
     "type" : "object",
     "title" : "Cache Control",
     "propertyOrder" : 9,
     "properties" : {
       "sun-idrepo-ldapv3-dncache-enabled" : {
         "title" : "DN Cache",
         "description" : "Used to enable/disable the DN Cache within the OpenAM repository
implementation.<br><br>The DN Cache is used to cache DN lookups which tend to happen in bursts during
authentication. The DN Cache can become out of date when a user is moved or renamed in the underlying
LDAP store and this is not reflected in a persistent search result. Enable when the underlying LDAP
store supports persistent search and move/rename (mod_dn) results are available.",
         "propertyOrder" : 5900,
         "required" : false,
         "type" : "boolean",
         "exampleValue" : ""
```

```
        },
        "sun-idrepo-ldapv3-dncache-size" : {
          "title" : "DN Cache Size",
          "description" : "In DN items, only used when DN Cache is enabled.",
          "propertyOrder" : 6000,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        }
      }
    },
    "errorhandling" : {
      "type" : "object",
      "title" : "Error Handling Configuration",
      "propertyOrder" : 8,
      "properties" : {
        "com.iplanet.am.ldap.connection.delay.between.retries" : {
          "title" : "The Delay Time Between Retries",
          "description" : "In milliseconds.",
          "propertyOrder" : 5800,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        }
      }
    },
    "groupconfig" : {
      "type" : "object",
      "title" : "Group Configuration",
      "propertyOrder" : 5,
      "properties" : {
        "sun-idrepo-ldapv3-config-groups-search-attribute" : {
          "title" : "LDAP Groups Search Attribute",
          "description" : "",
          "propertyOrder" : 2900,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-group-container-value" : {
          "title" : "LDAP Groups Container Value",
          "description" : "",
          "propertyOrder" : 3200,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-groups-search-filter" : {
          "title" : "LDAP Groups Search Filter",
          "description" : "",
          "propertyOrder" : 3000,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-uniquemember" : {
          "title" : "Attribute Name of Unique Member",
          "description" : "",
          "propertyOrder" : 3600,
```

```
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-group-objectclass" : {
          "title" : "LDAP Groups Object Class",
          "description" : "",
          "propertyOrder" : 3300,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-group-container-name" : {
          "title" : "LDAP Groups Container Naming Attribute",
          "description" : "",
          "propertyOrder" : 3100,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-memberurl" : {
          "title" : "Attribute Name of Group Member URL",
          "description" : "",
          "propertyOrder" : 3700,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-group-attributes" : {
          "title" : "LDAP Groups Attributes",
          "description" : "",
          "propertyOrder" : 3400,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-memberof" : {
          "title" : "Attribute Name for Group Membership",
          "description" : "",
          "propertyOrder" : 3500,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "authentication" : {
      "type" : "object",
      "title" : "Authentication Configuration",
      "propertyOrder" : 4,
      "properties" : {
        "sun-idrepo-ldapv3-config-auth-naming-attr" : {
          "title" : "Authentication Naming Attribute",
```

```
          "description" : "",
          "propertyOrder" : 5200,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "pluginconfig" : {
      "type" : "object",
      "title" : "Plug-in Configuration",
      "propertyOrder" : 2,
      "properties" : {
        "sunIdRepoSupportedOperations" : {
          "title" : "LDAPv3 Plug-in Supported Types and Operations",
          "description" : "",
          "propertyOrder" : 1900,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "sunIdRepoClass" : {
          "title" : "LDAPv3 Repository Plug-in Class Name",
          "description" : "",
          "propertyOrder" : 1700,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "sunIdRepoAttributeMapping" : {
          "title" : "Attribute Name Mapping",
          "description" : "",
          "propertyOrder" : 1800,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        }
      }
    }
  }
}
```

delete

Usage:

```
am> delete ForgeRockIAMDirectoryServer --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action ForgeRockIAMDirectoryServer --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action ForgeRockIAMDirectoryServer --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action ForgeRockIAMDirectoryServer --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query ForgeRockIAMDirectoryServer --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read ForgeRockIAMDirectoryServer --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update ForgeRockIAMDirectoryServer --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "userconfig" : {
      "type" : "object",
      "title" : "User Configuration",
      "propertyOrder" : 3,
      "properties" : {
        "sun-idrepo-ldapv3-config-people-container-name" : {
          "title" : "LDAP People Container Naming Attribute",
          "description" : "",
          "propertyOrder" : 5000,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-active" : {
          "title" : "User Status Active Value",
          "description" : "",
          "propertyOrder" : 2700,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-users-search-attribute" : {
          "title" : "LDAP Users  Search Attribute",
          "description" : "",
          "propertyOrder" : 2100,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-auth-kba-index-attr" : {
          "title" : "Knowledge Based Authentication Active Index",
          "description" : "",
          "propertyOrder" : 5400,
```

```
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-users-search-filter" : {
          "title" : "LDAP Users  Search Filter",
          "description" : "",
          "propertyOrder" : 2200,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-user-objectclass" : {
          "title" : "LDAP User Object Class",
          "description" : "",
          "propertyOrder" : 2300,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-createuser-attr-mapping" : {
          "title" : "Create User Attribute Mapping",
          "description" : "Format: attribute name or TargetAttributeName=SourceAttributeName",
          "propertyOrder" : 2500,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-auth-kba-attr" : {
          "title" : "Knowledge Based Authentication Attribute Name",
          "description" : "",
          "propertyOrder" : 5300,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-people-container-value" : {
          "title" : "LDAP People Container Value",
          "description" : "",
          "propertyOrder" : 5100,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-auth-kba-attempts-attr" : {
          "title" : "Knowledge Based Authentication Attempts Attribute Name",
          "description" : "",
          "propertyOrder" : 5410,
          "required" : false,
          "items" : {
```

```
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-inactive" : {
          "title" : "User Status Inactive Value",
          "description" : "",
          "propertyOrder" : 2800,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-user-attributes" : {
          "title" : "LDAP User Attributes",
          "description" : "",
          "propertyOrder" : 2400,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-isactive" : {
          "title" : "Attribute Name of User Status",
          "description" : "",
          "propertyOrder" : 2600,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "persistentsearch" : {
      "type" : "object",
      "title" : "Persistent Search Controls",
      "propertyOrder" : 7,
      "properties" : {
        "sun-idrepo-ldapv3-config-psearch-scope" : {
          "title" : "Persistent Search Scope",
          "description" : "",
          "propertyOrder" : 5700,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-psearch-filter" : {
          "title" : "Persistent Search Filter",
          "description" : "",
          "propertyOrder" : 5600,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-psearchbase" : {
          "title" : "Persistent Search Base DN",
          "description" : "",
          "propertyOrder" : 5500,
```

```
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "ldapsettings" : {
      "type" : "object",
      "title" : "Server Settings",
      "propertyOrder" : 0,
      "properties" : {
        "openam-idrepo-ldapv3-proxied-auth-denied-fallback" : {
          "title" : "Fallback using Bind DN if Proxied Authorization denied",
          "description" : "Enable this setting to fallback and retry using non-proxied authorization
(DS proxied-auth privilege) when proxied authorization is denied. Normally this happens when the
attributes cannot be changed because the account is locked or the password has expired. This setting
is effective only when Proxied Authorization is enabled.",
          "propertyOrder" : 860,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-connection-mode" : {
          "title" : "LDAP Connection Mode",
          "description" : "Defines which protocol/operation is used to establish the connection to
the LDAP Directory Server.<br><br>If 'LDAP' is selected, the connection <b>won't be secured</b> and
passwords are transferred in <b>cleartext</b> over the network.<br/> If 'LDAPS' is selected, the
connection is secured via SSL or TLS. <br/> If 'StartTLS' is selected, the connection is secured by
using StartTLS extended operation.",
          "propertyOrder" : 1000,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-max-result" : {
          "title" : "Maximum Results Returned from Search",
          "description" : "",
          "propertyOrder" : 1500,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-connection_pool_max_size" : {
          "title" : "LDAP Connection Pool Maximum Size",
          "description" : "",
          "propertyOrder" : 1200,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-time-limit" : {
          "title" : "Search Timeout",
          "description" : "In seconds.",
          "propertyOrder" : 1600,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-authid" : {
```

```
          "title" : "LDAP Bind DN",
          "description" : "A user or admin with sufficient access rights to perform the supported
operations.",
          "propertyOrder" : 700,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-connection_pool_min_size" : {
          "title" : "LDAP Connection Pool Minimum Size",
          "description" : "",
          "propertyOrder" : 1100,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "openam-idrepo-ldapv3-heartbeat-interval" : {
          "title" : "LDAP Connection Heartbeat Interval",
          "description" : "Specifies how often should OpenAM send a heartbeat request to the
directory.<br><br>This setting controls how often OpenAM <b>should</b> send a heartbeat search
request to the configured directory. If a connection becomes unresponsive (e.g. due to a network
error) then it may take up to the interval period before the problem is detected. Use along with the
Heartbeat Time Unit parameter to define the exact interval. Zero or negative value will result in
disabling heartbeat requests.",
          "propertyOrder" : 1300,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-authpw" : {
          "title" : "LDAP Bind Password",
          "description" : "",
          "propertyOrder" : 800,
          "required" : false,
          "type" : "string",
          "format" : "password",
          "exampleValue" : ""
        },
        "openam-idrepo-ldapv3-heartbeat-timeunit" : {
          "title" : "LDAP Connection Heartbeat Time Unit",
          "description" : "Defines the time unit corresponding to the Heartbeat Interval
setting.<br><br>This setting controls how often OpenAM <b>should</b> send a heartbeat search request
to the configured directory. If a connection becomes unresponsive (e.g. due to a network error) then
it may take up to the interval period before the problem is detected. Use along with the Heartbeat
Interval parameter to define the exact interval.",
          "propertyOrder" : 1400,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-search-scope" : {
          "title" : "LDAPv3 Plug-in Search Scope",
          "description" : "",
          "propertyOrder" : 2000,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "openam-idrepo-ldapv3-behera-support-enabled" : {
```

```
          "title" : "Behera Support Enabled",
          "description" : "When enabled, Behera draft control will be used in the outgoing requests
for operations that may modify password value. This will allow OpenAM to display password policy
related error messages when password policies are not met.",
          "propertyOrder" : 6100,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "openam-idrepo-ldapv3-affinity-enabled" : {
          "title" : "Affinity Enabled",
          "description" : "Enables affinity based request load balancing when accessing the user store
servers (based on DN). It is imperative that the connection string setting is set to the same value
for all OpenAM servers in the deployment when this feature is enabled.",
          "propertyOrder" : 6300,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-ldap-server" : {
          "title" : "LDAP Server",
          "description" : "Format: LDAP server host name:port | server_ID | site_ID",
          "propertyOrder" : 600,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "minItems" : 1,
          "type" : "array",
          "exampleValue" : ""
        },
        "openam-idrepo-ldapv3-proxied-auth-enabled" : {
          "title" : "Proxied Authorization using Bind DN",
          "description" : "Enable this setting if you have configured the LDAP bind DN account for
proxied authorization (DS proxied-auth privilege). Do not enable this property if the LDAP bind DN
account does not have the proxied-auth privilege granted because the user would not be able to reset
their password. DS and AM log an error when this occurs.",
          "propertyOrder" : 850,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-organization_name" : {
          "title" : "LDAP Organization DN",
          "description" : "",
          "propertyOrder" : 900,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "cachecontrol" : {
      "type" : "object",
      "title" : "Cache Control",
      "propertyOrder" : 9,
      "properties" : {
        "sun-idrepo-ldapv3-dncache-enabled" : {
          "title" : "DN Cache",
```

```
          "description" : "Used to enable/disable the DN Cache within the OpenAM repository
implementation.<br><br>The DN Cache is used to cache DN lookups which tend to happen in bursts during
authentication. The DN Cache can become out of date when a user is moved or renamed in the underlying
LDAP store and this is not reflected in a persistent search result. Enable when the underlying LDAP
store supports persistent search and move/rename (mod_dn) results are available.",
          "propertyOrder" : 5900,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-dncache-size" : {
          "title" : "DN Cache Size",
          "description" : "In DN items, only used when DN Cache is enabled.",
          "propertyOrder" : 6000,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        }
      }
    },
    "errorhandling" : {
      "type" : "object",
      "title" : "Error Handling Configuration",
      "propertyOrder" : 8,
      "properties" : {
        "com.iplanet.am.ldap.connection.delay.between.retries" : {
          "title" : "The Delay Time Between Retries",
          "description" : "In milliseconds.",
          "propertyOrder" : 5800,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        }
      }
    },
    "groupconfig" : {
      "type" : "object",
      "title" : "Group Configuration",
      "propertyOrder" : 5,
      "properties" : {
        "sun-idrepo-ldapv3-config-groups-search-attribute" : {
          "title" : "LDAP Groups Search Attribute",
          "description" : "",
          "propertyOrder" : 2900,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-group-container-value" : {
          "title" : "LDAP Groups Container Value",
          "description" : "",
          "propertyOrder" : 3200,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-groups-search-filter" : {
          "title" : "LDAP Groups Search Filter",
          "description" : "",
```

```
          "propertyOrder" : 3000,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-uniquemember" : {
          "title" : "Attribute Name of Unique Member",
          "description" : "",
          "propertyOrder" : 3600,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-group-objectclass" : {
          "title" : "LDAP Groups Object Class",
          "description" : "",
          "propertyOrder" : 3300,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-group-container-name" : {
          "title" : "LDAP Groups Container Naming Attribute",
          "description" : "",
          "propertyOrder" : 3100,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-memberurl" : {
          "title" : "Attribute Name of Group Member URL",
          "description" : "",
          "propertyOrder" : 3700,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-group-attributes" : {
          "title" : "LDAP Groups Attributes",
          "description" : "",
          "propertyOrder" : 3400,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-memberof" : {
          "title" : "Attribute Name for Group Membership",
          "description" : "",
          "propertyOrder" : 3500,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        }
```

```
      }
    },
    "authentication" : {
      "type" : "object",
      "title" : "Authentication Configuration",
      "propertyOrder" : 4,
      "properties" : {
        "sun-idrepo-ldapv3-config-auth-naming-attr" : {
          "title" : "Authentication Naming Attribute",
          "description" : "",
          "propertyOrder" : 5200,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "pluginconfig" : {
      "type" : "object",
      "title" : "Plug-in Configuration",
      "propertyOrder" : 2,
      "properties" : {
        "sunIdRepoSupportedOperations" : {
          "title" : "LDAPv3 Plug-in Supported Types and Operations",
          "description" : "",
          "propertyOrder" : 1900,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "sunIdRepoClass" : {
          "title" : "LDAPv3 Repository Plug-in Class Name",
          "description" : "",
          "propertyOrder" : 1700,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "sunIdRepoAttributeMapping" : {
          "title" : "Attribute Name Mapping",
          "description" : "",
          "propertyOrder" : 1800,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        }
      }
    }
  }
}
```

ForgottenPassword

Realm Operations

Self Service endpoint for retrieving a forgotten password

Resource path: `/selfservice/forgottenPassword`

Resource version: `1.0`

read

Initialise the forgotten password reclamation process.A set of requirements will be returned that will need to be fulfilled and sent to the submitRequirements action.

Usage:

```
am> read ForgottenPassword --realm Realm
```

submitRequirements

Submit some fulfilled requirements. Returns either a completion status, or a token along with some more requirements. If requirements are returned, they should be submitted with the token as a fresh request to this action.

Usage:

```
am> action ForgottenPassword --realm Realm --body body --actionName submitRequirements
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "$schema" : "http://json-schema.org/draft-04/schema#",
  "description" : "The structure of a request to the submitRequirements action.",
  "type" : "object",
  "title" : "Submit requirements structure",
  "properties" : {
    "token" : {
      "type" : "string",
      "title" : "Token",
      "description" : "The token returned from the previous submitRequirements request."
    },
    "input" : {
      "type" : "object",
      "title" : "Input",
      "description" : "The input as collected from the user that has forgotten their password. This
 object must conform to the JSON Schema of the requirements property from the last response.",
      "patternProperties" : {
        ".*" : {
          "type" : "any",
          "title" : "Input Property",
          "description" : "Valid content according to the received JSON Schema."
        }
      }
    }
  },
  "required" : [ "input" ]
}
```

ForgottenUsername

Realm Operations

Self Service endpoint for retrieving a forgotten username

Resource path: `/selfservice/forgottenUsername`

Resource version: `1.0`

read

Initialise the forgotten username reclamation process.A set of requirements will be returned that will need to be fulfilled and sent to the submitRequirements action.

Usage:

```
am> read ForgottenUsername --realm Realm
```

submitRequirements

Submit some fulfilled requirements. Returns either a completion status, or a token along with some more requirements. If requirements are returned, they should be submitted with the token as a fresh request to this action.

Usage:

```
am> action ForgottenUsername --realm Realm --body body --actionName submitRequirements
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "$schema" : "http://json-schema.org/draft-04/schema#",
  "description" : "The structure of a request to the submitRequirements action.",
  "type" : "object",
  "title" : "Submit requirements structure",
  "properties" : {
    "token" : {
      "type" : "string",
      "title" : "Token",
      "description" : "The token returned from the previous submitRequirements request."
    },
    "input" : {
      "type" : "object",
      "title" : "Input",
      "description" : "The input as collected from the user that has forgotten their username. This
 object must conform to the JSON Schema of the requirements property from the last response.",
      "patternProperties" : {
        ".*" : {
          "type" : "any",
          "title" : "Input Property",
          "description" : "Valid content according to the received JSON Schema."
        }
      }
    }
  },
  "required" : [ "input" ]
}
```

GeneralProperties

Global Operations

An object of property key-value pairs

Resource path: `/global-config/servers/{serverName}/properties/general`

Resource version: `1.0`

read

Usage:

```
am> read GeneralProperties --global --serverName serverName
```

Parameters:

--serverName

An object of property key-value pairs

update

Usage:

```
am> update GeneralProperties --global --serverName serverName --body body
```

Parameters:

--serverName

An object of property key-value pairs

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "amconfig.header.site" : {
      "title" : "Site",
      "type" : "object",
      "propertyOrder" : 0,
      "properties" : {
        "singleChoiceSite" : {
          "enum" : null,
          "options" : {
            "enum_titles" : null
          },
          "type" : "string",
          "title" : "Parent Site",
          "propertyOrder" : 0,
          "required" : false,
          "description" : "Parent Site"
        }
      }
    },
    "amconfig.header.installdir" : {
      "title" : "System",
      "type" : "object",
      "propertyOrder" : 1,
      "properties" : {
        "com.iplanet.services.configpath" : {
```

```
          "title" : "Base installation directory",
          "type" : "object",
          "propertyOrder" : 0,
          "description" : "Base directory where product's data resides. (property name:
com.iplanet.services.configpath)",
          "properties" : {
            "value" : {
              "type" : "string",
              "required" : false
            },
            "inherited" : {
              "type" : "boolean",
              "required" : true
            }
          }
        },
        "com.iplanet.am.locale" : {
          "title" : "Default Locale",
          "type" : "object",
          "propertyOrder" : 1,
          "description" : "Default locale for the product. (property name: com.iplanet.am.locale)",
          "properties" : {
            "value" : {
              "type" : "string",
              "required" : false
            },
            "inherited" : {
              "type" : "boolean",
              "required" : true
            }
          }
        },
        "com.sun.identity.client.notification.url" : {
          "title" : "Notification URL",
          "type" : "object",
          "propertyOrder" : 2,
          "description" : "The location of notification service end point. It is usually the product's
deployment URI/notificationservice. (property name: com.sun.identity.client.notification.url)",
          "properties" : {
            "value" : {
              "type" : "string",
              "required" : false
            },
            "inherited" : {
              "type" : "boolean",
              "required" : true
            }
          }
        },
        "com.iplanet.am.util.xml.validating" : {
          "title" : "XML Validation",
          "type" : "object",
          "propertyOrder" : 3,
          "description" : "Specifies if validation is required when parsing XML documents. (property
name: com.iplanet.am.util.xml.validating)",
          "properties" : {
            "value" : {
              "enum" : [ "on", "off" ],
              "options" : {
```

```
              "enum_titles" : [ "On", "Off" ]
            },
            "type" : "string",
            "required" : false
          },
          "inherited" : {
            "type" : "boolean",
            "required" : true
          }
        }
      }
    }
  },
  "amconfig.header.debug" : {
    "title" : "Debugging",
    "type" : "object",
    "propertyOrder" : 2,
    "properties" : {
      "com.iplanet.services.debug.level" : {
        "title" : "Debug Level",
        "type" : "object",
        "propertyOrder" : 0,
        "description" : "Debug level for all components in the product. (property name:
com.iplanet.services.debug.level)",
        "properties" : {
          "value" : {
            "enum" : [ "off", "error", "warning", "message" ],
            "options" : {
              "enum_titles" : [ "Off", "Error", "Warning", "Message" ]
            },
            "type" : "string",
            "required" : false
          },
          "inherited" : {
            "type" : "boolean",
            "required" : true
          }
        }
      },
      "com.sun.services.debug.mergeall" : {
        "title" : "Merge Debug Files",
        "type" : "object",
        "propertyOrder" : 1,
        "description" : "On : Directs all debug data to a single file (debug.out); Off : creates
separate per-component debug files (property name : com.sun.services.debug.mergeall)",
        "properties" : {
          "value" : {
            "enum" : [ "on", "off" ],
            "options" : {
              "enum_titles" : [ "On", "Off" ]
            },
            "type" : "string",
            "required" : false
          },
          "inherited" : {
            "type" : "boolean",
            "required" : true
          }
        }
```

```
      },
      "com.iplanet.services.debug.directory" : {
        "title" : "Debug Directory",
        "type" : "object",
        "propertyOrder" : 2,
        "description" : "Directory where debug files reside. (property name:
com.iplanet.services.debug.directory)",
        "properties" : {
          "value" : {
            "type" : "string",
            "required" : false
          },
          "inherited" : {
            "type" : "boolean",
            "required" : true
          }
        }
      }
    }
  },
  "amconfig.header.mailserver" : {
    "title" : "Mail Server",
    "type" : "object",
    "propertyOrder" : 3,
    "properties" : {
      "com.iplanet.am.smtphost" : {
        "title" : "Mail Server Host Name",
        "type" : "object",
        "propertyOrder" : 0,
        "description" : "(property name: com.iplanet.am.smtphost)",
        "properties" : {
          "value" : {
            "type" : "string",
            "required" : false
          },
          "inherited" : {
            "type" : "boolean",
            "required" : true
          }
        }
      },
      "com.iplanet.am.smtpport" : {
        "title" : "Mail Server Port Number",
        "type" : "object",
        "propertyOrder" : 1,
        "description" : "(property name: com.iplanet.am.smtpport)",
        "properties" : {
          "value" : {
            "type" : "integer",
            "required" : false
          },
          "inherited" : {
            "type" : "boolean",
            "required" : true
          }
        }
      }
    }
  }
```

```
  }
}
```

GenericLDAPv3

Realm Operations

Resource path: `/realm-config/services/id-repositories/LDAPv3`

Resource version: `1.0`

create

Usage:

```
am> create GenericLDAPv3 --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "groupconfig" : {
      "type" : "object",
      "title" : "Group Configuration",
      "propertyOrder" : 5,
      "properties" : {
        "sun-idrepo-ldapv3-config-group-attributes" : {
          "title" : "LDAP Groups Attributes",
          "description" : "",
          "propertyOrder" : 3400,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-group-objectclass" : {
          "title" : "LDAP Groups Object Class",
          "description" : "",
          "propertyOrder" : 3300,
          "required" : false,
```

```
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-memberurl" : {
          "title" : "Attribute Name of Group Member URL",
          "description" : "",
          "propertyOrder" : 3700,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-groups-search-filter" : {
          "title" : "LDAP Groups Search Filter",
          "description" : "",
          "propertyOrder" : 3000,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-memberof" : {
          "title" : "Attribute Name for Group Membership",
          "description" : "",
          "propertyOrder" : 3500,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-group-container-name" : {
          "title" : "LDAP Groups Container Naming Attribute",
          "description" : "",
          "propertyOrder" : 3100,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-dftgroupmember" : {
          "title" : "Default Group Member's User DN",
          "description" : "User automatically added when group is created.",
          "propertyOrder" : 3800,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-group-container-value" : {
          "title" : "LDAP Groups Container Value",
          "description" : "",
          "propertyOrder" : 3200,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-groups-search-attribute" : {
          "title" : "LDAP Groups Search Attribute",
          "description" : "",
          "propertyOrder" : 2900,
          "required" : false,
```

```
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-uniquemember" : {
          "title" : "Attribute Name of Unique Member",
          "description" : "",
          "propertyOrder" : 3600,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "userconfig" : {
      "type" : "object",
      "title" : "User Configuration",
      "propertyOrder" : 3,
      "properties" : {
        "sun-idrepo-ldapv3-config-user-attributes" : {
          "title" : "LDAP User Attributes",
          "description" : "",
          "propertyOrder" : 2400,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-isactive" : {
          "title" : "Attribute Name of User Status",
          "description" : "",
          "propertyOrder" : 2600,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-active" : {
          "title" : "User Status Active Value",
          "description" : "",
          "propertyOrder" : 2700,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-users-search-attribute" : {
          "title" : "LDAP Users  Search Attribute",
          "description" : "",
          "propertyOrder" : 2100,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-people-container-name" : {
          "title" : "LDAP People Container Naming Attribute",
          "description" : "",
          "propertyOrder" : 5000,
          "required" : false,
          "type" : "string",
```

```
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-auth-kba-attr" : {
          "title" : "Knowledge Based Authentication Attribute Name",
          "description" : "",
          "propertyOrder" : 5300,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-auth-kba-index-attr" : {
          "title" : "Knowledge Based Authentication Active Index",
          "description" : "",
          "propertyOrder" : 5400,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-createuser-attr-mapping" : {
          "title" : "Create User Attribute Mapping",
          "description" : "Format: attribute name or TargetAttributeName=SourceAttributeName",
          "propertyOrder" : 2500,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-inactive" : {
          "title" : "User Status Inactive Value",
          "description" : "",
          "propertyOrder" : 2800,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-user-objectclass" : {
          "title" : "LDAP User Object Class",
          "description" : "",
          "propertyOrder" : 2300,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-users-search-filter" : {
          "title" : "LDAP Users  Search Filter",
          "description" : "",
          "propertyOrder" : 2200,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
```

```
       "sun-idrepo-ldapv3-config-auth-kba-attempts-attr" : {
         "title" : "Knowledge Based Authentication Attempts Attribute Name",
         "description" : "",
         "propertyOrder" : 5340,
         "required" : false,
         "items" : {
           "type" : "string"
         },
         "type" : "array",
         "exampleValue" : ""
       },
       "sun-idrepo-ldapv3-config-people-container-value" : {
         "title" : "LDAP People Container Value",
         "description" : "",
         "propertyOrder" : 5100,
         "required" : false,
         "type" : "string",
         "exampleValue" : ""
       }
     }
   },
   "ldapsettings" : {
     "type" : "object",
     "title" : "Server Settings",
     "propertyOrder" : 0,
     "properties" : {
       "openam-idrepo-ldapv3-heartbeat-timeunit" : {
         "title" : "LDAP Connection Heartbeat Time Unit",
         "description" : "Defines the time unit corresponding to the Heartbeat Interval
setting.<br><br>This setting controls how often OpenAM <b>should</b> send a heartbeat search request
to the configured directory. If a connection becomes unresponsive (e.g. due to a network error) then
it may take up to the interval period before the problem is detected. Use along with the Heartbeat
Interval parameter to define the exact interval.",
         "propertyOrder" : 1400,
         "required" : false,
         "type" : "string",
         "exampleValue" : ""
       },
       "sun-idrepo-ldapv3-config-authid" : {
         "title" : "LDAP Bind DN",
         "description" : "A user or admin with sufficient access rights to perform the supported
operations.",
         "propertyOrder" : 700,
         "required" : false,
         "type" : "string",
         "exampleValue" : ""
       },
       "sun-idrepo-ldapv3-config-ldap-server" : {
         "title" : "LDAP Server",
         "description" : "Format: LDAP server host name:port | server_ID | site_ID",
         "propertyOrder" : 600,
         "required" : true,
         "items" : {
           "type" : "string"
         },
         "minItems" : 1,
         "type" : "array",
         "exampleValue" : ""
       },
```

```
       "sun-idrepo-ldapv3-config-search-scope" : {
         "title" : "LDAPv3 Plug-in Search Scope",
         "description" : "",
         "propertyOrder" : 2000,
         "required" : false,
         "type" : "string",
         "exampleValue" : ""
       },
       "sun-idrepo-ldapv3-config-connection_pool_min_size" : {
         "title" : "LDAP Connection Pool Minimum Size",
         "description" : "",
         "propertyOrder" : 1100,
         "required" : false,
         "type" : "integer",
         "exampleValue" : ""
       },
       "sun-idrepo-ldapv3-config-connection-mode" : {
         "title" : "LDAP Connection Mode",
         "description" : "Defines which protocol/operation is used to establish the connection to
the LDAP Directory Server.<br><br>If 'LDAP' is selected, the connection <b>won't be secured</b> and
passwords are transferred in <b>cleartext</b> over the network.<br/> If 'LDAPS' is selected, the
connection is secured via SSL or TLS. <br/> If 'StartTLS' is selected, the connection is secured by
using StartTLS extended operation.",
         "propertyOrder" : 1000,
         "required" : false,
         "type" : "string",
         "exampleValue" : ""
       },
       "sun-idrepo-ldapv3-config-max-result" : {
         "title" : "Maximum Results Returned from Search",
         "description" : "",
         "propertyOrder" : 1500,
         "required" : false,
         "type" : "integer",
         "exampleValue" : ""
       },
       "sun-idrepo-ldapv3-config-authpw" : {
         "title" : "LDAP Bind Password",
         "description" : "",
         "propertyOrder" : 800,
         "required" : false,
         "type" : "string",
         "format" : "password",
         "exampleValue" : ""
       },
       "openam-idrepo-ldapv3-behera-support-enabled" : {
         "title" : "Behera Support Enabled",
         "description" : "When enabled, Behera draft control will be used in the outgoing requests
for operations that may modify password value. This will allow OpenAM to display password policy
related error messages when password policies are not met.",
         "propertyOrder" : 6100,
         "required" : false,
         "type" : "boolean",
         "exampleValue" : ""
       },
       "sun-idrepo-ldapv3-config-organization_name" : {
         "title" : "LDAP Organization DN",
         "description" : "",
         "propertyOrder" : 900,
```

```
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "openam-idrepo-ldapv3-affinity-enabled" : {
          "title" : "Affinity Enabled",
          "description" : "Enables affinity based request load balancing when accessing the user store
servers (based on DN). It is imperative that the connection string setting is set to the same value
for all OpenAM servers in the deployment when this feature is enabled.",
          "propertyOrder" : 6200,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "openam-idrepo-ldapv3-heartbeat-interval" : {
          "title" : "LDAP Connection Heartbeat Interval",
          "description" : "Specifies how often should OpenAM send a heartbeat request to the
directory.<br><br>This setting controls how often OpenAM <b>should</b> send a heartbeat search
request to the configured directory. If a connection becomes unresponsive (e.g. due to a network
error) then it may take up to the interval period before the problem is detected. Use along with the
Heartbeat Time Unit parameter to define the exact interval. Zero or negative value will result in
disabling heartbeat requests.",
          "propertyOrder" : 1300,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-connection_pool_max_size" : {
          "title" : "LDAP Connection Pool Maximum Size",
          "description" : "",
          "propertyOrder" : 1200,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-time-limit" : {
          "title" : "Search Timeout",
          "description" : "In seconds.",
          "propertyOrder" : 1600,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        }
      }
    },
    "persistentsearch" : {
      "type" : "object",
      "title" : "Persistent Search Controls",
      "propertyOrder" : 7,
      "properties" : {
        "sun-idrepo-ldapv3-config-psearch-scope" : {
          "title" : "Persistent Search Scope",
          "description" : "",
          "propertyOrder" : 5700,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-psearch-filter" : {
```

```
        "title" : "Persistent Search Filter",
        "description" : "",
        "propertyOrder" : 5600,
        "required" : false,
        "type" : "string",
        "exampleValue" : ""
      },
      "sun-idrepo-ldapv3-config-psearchbase" : {
        "title" : "Persistent Search Base DN",
        "description" : "",
        "propertyOrder" : 5500,
        "required" : false,
        "type" : "string",
        "exampleValue" : ""
      }
    }
  },
  "errorhandling" : {
    "type" : "object",
    "title" : "Error Handling Configuration",
    "propertyOrder" : 8,
    "properties" : {
      "com.iplanet.am.ldap.connection.delay.between.retries" : {
        "title" : "The Delay Time Between Retries",
        "description" : "In milliseconds.",
        "propertyOrder" : 5800,
        "required" : false,
        "type" : "integer",
        "exampleValue" : ""
      }
    }
  },
  "pluginconfig" : {
    "type" : "object",
    "title" : "Plug-in Configuration",
    "propertyOrder" : 2,
    "properties" : {
      "sunIdRepoSupportedOperations" : {
        "title" : "LDAPv3 Plug-in Supported Types and Operations",
        "description" : "",
        "propertyOrder" : 1900,
        "required" : false,
        "items" : {
          "type" : "string"
        },
        "type" : "array",
        "exampleValue" : ""
      },
      "sunIdRepoAttributeMapping" : {
        "title" : "Attribute Name Mapping",
        "description" : "",
        "propertyOrder" : 1800,
        "required" : false,
        "items" : {
          "type" : "string"
        },
        "type" : "array",
        "exampleValue" : ""
      },
```

```
        "sunIdRepoClass" : {
          "title" : "LDAPv3 Repository Plug-in Class Name",
          "description" : "",
          "propertyOrder" : 1700,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "cachecontrol" : {
      "type" : "object",
      "title" : "Cache Control",
      "propertyOrder" : 9,
      "properties" : {
        "sun-idrepo-ldapv3-dncache-enabled" : {
          "title" : "DN Cache",
          "description" : "Used to enable/disable the DN Cache within the OpenAM repository
 implementation.<br><br>The DN Cache is used to cache DN lookups which tend to happen in bursts during
 authentication. The DN Cache can become out of date when a user is moved or renamed in the underlying
 LDAP store and this is not reflected in a persistent search result. Enable when the underlying LDAP
 store supports persistent search and move/rename (mod_dn) results are available.",
          "propertyOrder" : 5900,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-dncache-size" : {
          "title" : "DN Cache Size",
          "description" : "In DN items, only used when DN Cache is enabled.",
          "propertyOrder" : 6000,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        }
      }
    },
    "authentication" : {
      "type" : "object",
      "title" : "Authentication Configuration",
      "propertyOrder" : 4,
      "properties" : {
        "sun-idrepo-ldapv3-config-auth-naming-attr" : {
          "title" : "Authentication Naming Attribute",
          "description" : "",
          "propertyOrder" : 5200,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    }
  }
}
```

delete

Usage:

```
am> delete GenericLDAPv3 --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action GenericLDAPv3 --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action GenericLDAPv3 --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action GenericLDAPv3 --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query GenericLDAPv3 --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read GenericLDAPv3 --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update GenericLDAPv3 --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "groupconfig" : {
      "type" : "object",
      "title" : "Group Configuration",
      "propertyOrder" : 5,
      "properties" : {
        "sun-idrepo-ldapv3-config-group-attributes" : {
          "title" : "LDAP Groups Attributes",
          "description" : "",
          "propertyOrder" : 3400,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-group-objectclass" : {
          "title" : "LDAP Groups Object Class",
          "description" : "",
          "propertyOrder" : 3300,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
```

```
        "sun-idrepo-ldapv3-config-memberurl" : {
          "title" : "Attribute Name of Group Member URL",
          "description" : "",
          "propertyOrder" : 3700,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-groups-search-filter" : {
          "title" : "LDAP Groups Search Filter",
          "description" : "",
          "propertyOrder" : 3000,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-memberof" : {
          "title" : "Attribute Name for Group Membership",
          "description" : "",
          "propertyOrder" : 3500,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-group-container-name" : {
          "title" : "LDAP Groups Container Naming Attribute",
          "description" : "",
          "propertyOrder" : 3100,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-dftgroupmember" : {
          "title" : "Default Group Member's User DN",
          "description" : "User automatically added when group is created.",
          "propertyOrder" : 3800,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-group-container-value" : {
          "title" : "LDAP Groups Container Value",
          "description" : "",
          "propertyOrder" : 3200,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-groups-search-attribute" : {
          "title" : "LDAP Groups Search Attribute",
          "description" : "",
          "propertyOrder" : 2900,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-uniquemember" : {
          "title" : "Attribute Name of Unique Member",
          "description" : "",
```

```
        "propertyOrder" : 3600,
        "required" : false,
        "type" : "string",
        "exampleValue" : ""
      }
    }
  },
  "userconfig" : {
    "type" : "object",
    "title" : "User Configuration",
    "propertyOrder" : 3,
    "properties" : {
      "sun-idrepo-ldapv3-config-user-attributes" : {
        "title" : "LDAP User Attributes",
        "description" : "",
        "propertyOrder" : 2400,
        "required" : false,
        "items" : {
          "type" : "string"
        },
        "type" : "array",
        "exampleValue" : ""
      },
      "sun-idrepo-ldapv3-config-isactive" : {
        "title" : "Attribute Name of User Status",
        "description" : "",
        "propertyOrder" : 2600,
        "required" : false,
        "type" : "string",
        "exampleValue" : ""
      },
      "sun-idrepo-ldapv3-config-active" : {
        "title" : "User Status Active Value",
        "description" : "",
        "propertyOrder" : 2700,
        "required" : false,
        "type" : "string",
        "exampleValue" : ""
      },
      "sun-idrepo-ldapv3-config-users-search-attribute" : {
        "title" : "LDAP Users  Search Attribute",
        "description" : "",
        "propertyOrder" : 2100,
        "required" : false,
        "type" : "string",
        "exampleValue" : ""
      },
      "sun-idrepo-ldapv3-config-people-container-name" : {
        "title" : "LDAP People Container Naming Attribute",
        "description" : "",
        "propertyOrder" : 5000,
        "required" : false,
        "type" : "string",
        "exampleValue" : ""
      },
      "sun-idrepo-ldapv3-config-auth-kba-attr" : {
        "title" : "Knowledge Based Authentication Attribute Name",
        "description" : "",
        "propertyOrder" : 5300,
```

```
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-auth-kba-index-attr" : {
          "title" : "Knowledge Based Authentication Active Index",
          "description" : "",
          "propertyOrder" : 5400,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-createuser-attr-mapping" : {
          "title" : "Create User Attribute Mapping",
          "description" : "Format: attribute name or TargetAttributeName=SourceAttributeName",
          "propertyOrder" : 2500,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-inactive" : {
          "title" : "User Status Inactive Value",
          "description" : "",
          "propertyOrder" : 2800,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-user-objectclass" : {
          "title" : "LDAP User Object Class",
          "description" : "",
          "propertyOrder" : 2300,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-users-search-filter" : {
          "title" : "LDAP Users  Search Filter",
          "description" : "",
          "propertyOrder" : 2200,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-auth-kba-attempts-attr" : {
          "title" : "Knowledge Based Authentication Attempts Attribute Name",
          "description" : "",
          "propertyOrder" : 5340,
          "required" : false,
          "items" : {
```

```
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-people-container-value" : {
          "title" : "LDAP People Container Value",
          "description" : "",
          "propertyOrder" : 5100,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "ldapsettings" : {
      "type" : "object",
      "title" : "Server Settings",
      "propertyOrder" : 0,
      "properties" : {
        "openam-idrepo-ldapv3-heartbeat-timeunit" : {
          "title" : "LDAP Connection Heartbeat Time Unit",
          "description" : "Defines the time unit corresponding to the Heartbeat Interval
setting.<br><br>This setting controls how often OpenAM <b>should</b> send a heartbeat search request
to the configured directory. If a connection becomes unresponsive (e.g. due to a network error) then
it may take up to the interval period before the problem is detected. Use along with the Heartbeat
Interval parameter to define the exact interval.",
          "propertyOrder" : 1400,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-authid" : {
          "title" : "LDAP Bind DN",
          "description" : "A user or admin with sufficient access rights to perform the supported
operations.",
          "propertyOrder" : 700,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-ldap-server" : {
          "title" : "LDAP Server",
          "description" : "Format: LDAP server host name:port | server_ID | site_ID",
          "propertyOrder" : 600,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "minItems" : 1,
          "type" : "array",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-search-scope" : {
          "title" : "LDAPv3 Plug-in Search Scope",
          "description" : "",
          "propertyOrder" : 2000,
          "required" : false,
          "type" : "string",
```

```
        "exampleValue" : ""
      },
      "sun-idrepo-ldapv3-config-connection_pool_min_size" : {
        "title" : "LDAP Connection Pool Minimum Size",
        "description" : "",
        "propertyOrder" : 1100,
        "required" : false,
        "type" : "integer",
        "exampleValue" : ""
      },
      "sun-idrepo-ldapv3-config-connection-mode" : {
        "title" : "LDAP Connection Mode",
        "description" : "Defines which protocol/operation is used to establish the connection to
the LDAP Directory Server.<br><br>If 'LDAP' is selected, the connection <b>won't be secured</b> and
passwords are transferred in <b>cleartext</b> over the network.<br/> If 'LDAPS' is selected, the
connection is secured via SSL or TLS. <br/> If 'StartTLS' is selected, the connection is secured by
using StartTLS extended operation.",
        "propertyOrder" : 1000,
        "required" : false,
        "type" : "string",
        "exampleValue" : ""
      },
      "sun-idrepo-ldapv3-config-max-result" : {
        "title" : "Maximum Results Returned from Search",
        "description" : "",
        "propertyOrder" : 1500,
        "required" : false,
        "type" : "integer",
        "exampleValue" : ""
      },
      "sun-idrepo-ldapv3-config-authpw" : {
        "title" : "LDAP Bind Password",
        "description" : "",
        "propertyOrder" : 800,
        "required" : false,
        "type" : "string",
        "format" : "password",
        "exampleValue" : ""
      },
      "openam-idrepo-ldapv3-behera-support-enabled" : {
        "title" : "Behera Support Enabled",
        "description" : "When enabled, Behera draft control will be used in the outgoing requests
for operations that may modify password value. This will allow OpenAM to display password policy
related error messages when password policies are not met.",
        "propertyOrder" : 6100,
        "required" : false,
        "type" : "boolean",
        "exampleValue" : ""
      },
      "sun-idrepo-ldapv3-config-organization_name" : {
        "title" : "LDAP Organization DN",
        "description" : "",
        "propertyOrder" : 900,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
      },
      "openam-idrepo-ldapv3-affinity-enabled" : {
        "title" : "Affinity Enabled",
```

```
          "description" : "Enables affinity based request load balancing when accessing the user store
servers (based on DN). It is imperative that the connection string setting is set to the same value
for all OpenAM servers in the deployment when this feature is enabled.",
          "propertyOrder" : 6200,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "openam-idrepo-ldapv3-heartbeat-interval" : {
          "title" : "LDAP Connection Heartbeat Interval",
          "description" : "Specifies how often should OpenAM send a heartbeat request to the
directory.<br><br>This setting controls how often OpenAM <b>should</b> send a heartbeat search
request to the configured directory. If a connection becomes unresponsive (e.g. due to a network
error) then it may take up to the interval period before the problem is detected. Use along with the
Heartbeat Time Unit parameter to define the exact interval. Zero or negative value will result in
disabling heartbeat requests.",
          "propertyOrder" : 1300,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-connection_pool_max_size" : {
          "title" : "LDAP Connection Pool Maximum Size",
          "description" : "",
          "propertyOrder" : 1200,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-time-limit" : {
          "title" : "Search Timeout",
          "description" : "In seconds.",
          "propertyOrder" : 1600,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        }
      }
    },
    "persistentsearch" : {
      "type" : "object",
      "title" : "Persistent Search Controls",
      "propertyOrder" : 7,
      "properties" : {
        "sun-idrepo-ldapv3-config-psearch-scope" : {
          "title" : "Persistent Search Scope",
          "description" : "",
          "propertyOrder" : 5700,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-psearch-filter" : {
          "title" : "Persistent Search Filter",
          "description" : "",
          "propertyOrder" : 5600,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
```

```
        },
        "sun-idrepo-ldapv3-config-psearchbase" : {
          "title" : "Persistent Search Base DN",
          "description" : "",
          "propertyOrder" : 5500,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "errorhandling" : {
      "type" : "object",
      "title" : "Error Handling Configuration",
      "propertyOrder" : 8,
      "properties" : {
        "com.iplanet.am.ldap.connection.delay.between.retries" : {
          "title" : "The Delay Time Between Retries",
          "description" : "In milliseconds.",
          "propertyOrder" : 5800,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        }
      }
    },
    "pluginconfig" : {
      "type" : "object",
      "title" : "Plug-in Configuration",
      "propertyOrder" : 2,
      "properties" : {
        "sunIdRepoSupportedOperations" : {
          "title" : "LDAPv3 Plug-in Supported Types and Operations",
          "description" : "",
          "propertyOrder" : 1900,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "sunIdRepoAttributeMapping" : {
          "title" : "Attribute Name Mapping",
          "description" : "",
          "propertyOrder" : 1800,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "sunIdRepoClass" : {
          "title" : "LDAPv3 Repository Plug-in Class Name",
          "description" : "",
          "propertyOrder" : 1700,
          "required" : true,
          "type" : "string",
```

```
          "exampleValue" : ""
        }
      }
    },
    "cachecontrol" : {
      "type" : "object",
      "title" : "Cache Control",
      "propertyOrder" : 9,
      "properties" : {
        "sun-idrepo-ldapv3-dncache-enabled" : {
          "title" : "DN Cache",
          "description" : "Used to enable/disable the DN Cache within the OpenAM repository
 implementation.<br><br>The DN Cache is used to cache DN lookups which tend to happen in bursts during
 authentication. The DN Cache can become out of date when a user is moved or renamed in the underlying
 LDAP store and this is not reflected in a persistent search result. Enable when the underlying LDAP
 store supports persistent search and move/rename (mod_dn) results are available.",
          "propertyOrder" : 5900,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-dncache-size" : {
          "title" : "DN Cache Size",
          "description" : "In DN items, only used when DN Cache is enabled.",
          "propertyOrder" : 6000,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        }
      }
    },
    "authentication" : {
      "type" : "object",
      "title" : "Authentication Configuration",
      "propertyOrder" : 4,
      "properties" : {
        "sun-idrepo-ldapv3-config-auth-naming-attr" : {
          "title" : "Authentication Naming Attribute",
          "description" : "",
          "propertyOrder" : 5200,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    }
  }
}
```

GetSessionData

Realm Operations

Resource path: `/realm-config/authentication/authenticationtrees/nodes/SessionDataNode`

Resource version: `1.0`

create

Usage:

```
am> create GetSessionData --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "sessionDataKey" : {
      "title" : "Session Data Key",
      "description" : "",
      "propertyOrder" : 100,
      "type" : "string",
      "exampleValue" : ""
    },
    "sharedStateKey" : {
      "title" : "Shared State Key",
      "description" : "",
      "propertyOrder" : 200,
      "type" : "string",
      "exampleValue" : ""
    }
  },
  "required" : [ "sessionDataKey", "sharedStateKey" ]
}
```

delete

Usage:

```
am> delete GetSessionData --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action GetSessionData --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action GetSessionData --realm Realm --actionName getCreatableTypes
```

listOutcomes

List the available outcomes for the node type.

Usage:

```
am> action GetSessionData --realm Realm --body body --actionName listOutcomes
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "title" : "Some configuration of the node. This does not need to be complete against the
 configuration schema."
}
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action GetSessionData --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query GetSessionData --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read GetSessionData --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update GetSessionData --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "sessionDataKey" : {
      "title" : "Session Data Key",
      "description" : "",
      "propertyOrder" : 100,
      "type" : "string",
      "exampleValue" : ""
    },
    "sharedStateKey" : {
      "title" : "Shared State Key",
      "description" : "",
      "propertyOrder" : 200,
      "type" : "string",
      "exampleValue" : ""
    }
  },
  "required" : [ "sessionDataKey", "sharedStateKey" ]
}
```

GlobalScripts

Global Operations

Resource path: `/global-config/services/scripting/globalScript`

Resource version: `1.0`

create

Usage:

```
am> create GlobalScripts --global --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "script" : {
      "title" : "Script",
      "description" : "The source code of the script. The source code is in UTF-8 format and encoded
 into Base64",
      "propertyOrder" : null,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "context" : {
      "title" : "Script type",
      "description" : "The script type. Supported values are: POLICY_CONDITION : Policy Condition
 AUTHENTICATION_SERVER_SIDE : Server-side Authentication  AUTHENTICATION_CLIENT_SIDE : Client-side
 Authentication - Note Client-side scripts must be written in JavaScript OIDC_CLAIMS : OIDC Claims
 SOCIAL_IDP_PROFILE_TRANSFORMATION : Social Identity Provider Profile Transformation",
      "propertyOrder" : null,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "lastModifiedDate" : {
      "title" : "Last modification date",
      "description" : "A string containing the last modified date and time, in ISO 8601 format. If
 the script has not been modified since it was created, this property will have the same value as
 creationDate",
      "propertyOrder" : null,
```

```
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "name" : {
      "title" : "Script name",
      "description" : "The name provided for the script",
      "propertyOrder" : null,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "createdBy" : {
      "title" : "Created by",
      "description" : "A string containing the universal identifier DN of the subject that created the
 script",
      "propertyOrder" : null,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "description" : {
      "title" : "Script description",
      "description" : "An optional text string to help identify the script",
      "propertyOrder" : null,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "lastModifiedBy" : {
      "title" : "Last modifier",
      "description" : "A string containing the universal identifier DN of the subject that most
 recently updated the script. If the script has not been modified since it was created, this property
 will have the same value as createdBy",
      "propertyOrder" : null,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "language" : {
      "title" : "Script language",
      "description" : "The language the script is written in - JAVASCRIPT or GROOVY",
      "propertyOrder" : null,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "creationDate" : {
      "title" : "Creation date",
      "description" : "An integer containing the creation date and time, in ISO 8601 format",
      "propertyOrder" : null,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
```

delete

Usage:

```
am> delete GlobalScripts --global --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action GlobalScripts --global --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action GlobalScripts --global --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action GlobalScripts --global --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query GlobalScripts --global --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read GlobalScripts --global --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update GlobalScripts --global --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "script" : {
      "title" : "Script",
      "description" : "The source code of the script. The source code is in UTF-8 format and encoded
 into Base64",
      "propertyOrder" : null,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "context" : {
      "title" : "Script type",
      "description" : "The script type. Supported values are: POLICY_CONDITION : Policy Condition
 AUTHENTICATION_SERVER_SIDE : Server-side Authentication  AUTHENTICATION_CLIENT_SIDE : Client-side
 Authentication - Note Client-side scripts must be written in JavaScript OIDC_CLAIMS : OIDC Claims
 SOCIAL_IDP_PROFILE_TRANSFORMATION : Social Identity Provider Profile Transformation",
      "propertyOrder" : null,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "lastModifiedDate" : {
      "title" : "Last modification date",
```

```
     "description" : "A string containing the last modified date and time, in ISO 8601 format. If
the script has not been modified since it was created, this property will have the same value as
creationDate",
     "propertyOrder" : null,
     "required" : true,
     "type" : "string",
     "exampleValue" : ""
   },
   "name" : {
     "title" : "Script name",
     "description" : "The name provided for the script",
     "propertyOrder" : null,
     "required" : true,
     "type" : "string",
     "exampleValue" : ""
   },
   "createdBy" : {
     "title" : "Created by",
     "description" : "A string containing the universal identifier DN of the subject that created the
script",
     "propertyOrder" : null,
     "required" : true,
     "type" : "string",
     "exampleValue" : ""
   },
   "description" : {
     "title" : "Script description",
     "description" : "An optional text string to help identify the script",
     "propertyOrder" : null,
     "required" : true,
     "type" : "string",
     "exampleValue" : ""
   },
   "lastModifiedBy" : {
     "title" : "Last modifier",
     "description" : "A string containing the universal identifier DN of the subject that most
recently updated the script. If the script has not been modified since it was created, this property
will have the same value as createdBy",
     "propertyOrder" : null,
     "required" : true,
     "type" : "string",
     "exampleValue" : ""
   },
   "language" : {
     "title" : "Script language",
     "description" : "The language the script is written in - JAVASCRIPT or GROOVY",
     "propertyOrder" : null,
     "required" : true,
     "type" : "string",
     "exampleValue" : ""
   },
   "creationDate" : {
     "title" : "Creation date",
     "description" : "An integer containing the creation date and time, in ISO 8601 format",
     "propertyOrder" : null,
     "required" : true,
     "type" : "string",
     "exampleValue" : ""
   }
```

```
  }
}
```

GlobalSecretsSettings

Global Operations

Resource path: `/global-config/secrets/GlobalSecrets`

Resource version: `1.0`

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action GlobalSecretsSettings --global --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action GlobalSecretsSettings --global --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action GlobalSecretsSettings --global --actionName nextdescendents
```

read

Usage:

```
am> read GlobalSecretsSettings --global
```

update

Usage:

```
am> update GlobalSecretsSettings --global --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "storeTypes" : {
      "title" : "Store types",
      "description" : "This setting contains the currently installed secrets store types.",
      "propertyOrder" : 100,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    }
  }
}
```

Globalization

Realm Operations

Resource path: `/realm-config/services/globalization`

Resource version: `1.0`

create

Usage:

```
am> create Globalization --realm Realm --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "commonNameFormats" : {
      "title" : "Auto Generated Common Name Format",
      "description" : "Use this list to configure how OpenAM formats names shown in the console
 banner.<br><br>This setting allows the name of the authenticated user shown in the OpenAM console
 banner to be customised based on the locale of the user.",
      "propertyOrder" : 300,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    }
  }
}
```

delete

Usage:

```
am> delete Globalization --realm Realm
```

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action Globalization --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action Globalization --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action Globalization --realm Realm --actionName nextdescendents
```

read

Usage:

```
am> read Globalization --realm Realm
```

update

Usage:

```
am> update Globalization --realm Realm --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "commonNameFormats" : {
      "title" : "Auto Generated Common Name Format",
      "description" : "Use this list to configure how OpenAM formats names shown in the console
 banner.<br><br>This setting allows the name of the authenticated user shown in the OpenAM console
 banner to be customised based on the locale of the user.",
      "propertyOrder" : 300,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    }
  }
}
```

Global Operations

Resource path: `/global-config/services/globalization`

Resource version: `1.0`

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action Globalization --global --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action Globalization --global --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action Globalization --global --actionName nextdescendents
```

read

Usage:

```
am> read Globalization --global
```

update

Usage:

```
am> update Globalization --global --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "sun-identity-g11n-settings-charset-alias-mapping" : {
      "title" : "Charset Aliases",
      "description" : "Use this list to map between different character set names used in Java and in
 MIME.",
      "propertyOrder" : 200,
```

```
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "charsetMappings" : {
      "title" : "Charsets Supported by Each Locale",
      "description" : "This table lets you configure the order of supported character sets used for
 each supported locale. Change the settings only if the defaults are not appropriate.",
      "propertyOrder" : 100,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "defaults" : {
      "properties" : {
        "commonNameFormats" : {
          "title" : "Auto Generated Common Name Format",
          "description" : "Use this list to configure how OpenAM formats names shown in the console
 banner.<br><br>This setting allows the name of the authenticated user shown in the OpenAM console
 banner to be customised based on the locale of the user.",
          "propertyOrder" : 300,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        }
      },
      "type" : "object",
      "title" : "Realm Defaults"
    }
  }
}
```

GoogleKeyManagementServiceSecretStore

Realm Operations

Resource path: `/realm-config/secrets/stores/GoogleKeyManagementServiceSecretStore`

Resource version: `1.0`

create

Usage:

```
am> create GoogleKeyManagementServiceSecretStore --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "project" : {
      "title" : "Project",
      "description" : "The GCP project that contains the key ring",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "location" : {
      "title" : "Location",
      "description" : "The <a href=\"https://cloud.google.com/kms/docs/locations\">GCP KMS location</
a>",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "publicKeyCacheMaxSize" : {
      "title" : "Public key cache size",
      "description" : "The maximum number of public keys to cache. The cache is per-server.",
      "propertyOrder" : 500,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "keyRing" : {
      "title" : "Key Ring",
      "description" : "The KMS key ring that contains the keys you want to use",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "publicKeyCacheDuration" : {
      "title" : "Public key cache duration (seconds)",
      "description" : "The length of time to cache public keys (default is 1 hour).",
      "propertyOrder" : 400,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
```

```
    }
  }
}
```

delete

Usage:

```
am> delete GoogleKeyManagementServiceSecretStore --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action GoogleKeyManagementServiceSecretStore --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action GoogleKeyManagementServiceSecretStore --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action GoogleKeyManagementServiceSecretStore --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query GoogleKeyManagementServiceSecretStore --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read GoogleKeyManagementServiceSecretStore --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update GoogleKeyManagementServiceSecretStore --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "project" : {
      "title" : "Project",
      "description" : "The GCP project that contains the key ring",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "location" : {
      "title" : "Location",
```

```
      "description" : "The <a href=\"https://cloud.google.com/kms/docs/locations\">GCP KMS location</
a>",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "publicKeyCacheMaxSize" : {
      "title" : "Public key cache size",
      "description" : "The maximum number of public keys to cache. The cache is per-server.",
      "propertyOrder" : 500,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "keyRing" : {
      "title" : "Key Ring",
      "description" : "The KMS key ring that contains the keys you want to use",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "publicKeyCacheDuration" : {
      "title" : "Public key cache duration (seconds)",
      "description" : "The length of time to cache public keys (default is 1 hour).",
      "propertyOrder" : 400,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    }
  }
}
```

Global Operations

Resource path: `/global-config/secrets/stores/GoogleKeyManagementServiceSecretStore`

Resource version: `1.0`

create

Usage:

```
am> create GoogleKeyManagementServiceSecretStore --global --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "publicKeyCacheMaxSize" : {
      "title" : "Public key cache size",
      "description" : "The maximum number of public keys to cache. The cache is per-server.",
      "propertyOrder" : 500,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "publicKeyCacheDuration" : {
      "title" : "Public key cache duration (seconds)",
      "description" : "The length of time to cache public keys (default is 1 hour).",
      "propertyOrder" : 400,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "location" : {
      "title" : "Location",
      "description" : "The <a href=\"https://cloud.google.com/kms/docs/locations\">GCP KMS location</
a>",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "project" : {
      "title" : "Project",
      "description" : "The GCP project that contains the key ring",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "keyRing" : {
      "title" : "Key Ring",
      "description" : "The KMS key ring that contains the keys you want to use",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
```

delete

Usage:

```
am> delete GoogleKeyManagementServiceSecretStore --global --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action GoogleKeyManagementServiceSecretStore --global --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action GoogleKeyManagementServiceSecretStore --global --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action GoogleKeyManagementServiceSecretStore --global --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query GoogleKeyManagementServiceSecretStore --global --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read GoogleKeyManagementServiceSecretStore --global --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update GoogleKeyManagementServiceSecretStore --global --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "publicKeyCacheMaxSize" : {
      "title" : "Public key cache size",
      "description" : "The maximum number of public keys to cache. The cache is per-server.",
      "propertyOrder" : 500,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "publicKeyCacheDuration" : {
      "title" : "Public key cache duration (seconds)",
      "description" : "The length of time to cache public keys (default is 1 hour).",
      "propertyOrder" : 400,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "location" : {
      "title" : "Location",
      "description" : "The <a href=\"https://cloud.google.com/kms/docs/locations\">GCP KMS location</
a>",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
```

```
    "project" : {
      "title" : "Project",
      "description" : "The GCP project that contains the key ring",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "keyRing" : {
      "title" : "Key Ring",
      "description" : "The KMS key ring that contains the keys you want to use",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
```

GoogleKmsMappings

Realm Operations

Resource path: `/realm-config/secrets/stores/GoogleKeyManagementServiceSecretStore/{GoogleKeyManagementServiceSecretStore}/mappings`

Resource version: `1.0`

create

Usage:

```
am> create GoogleKmsMappings --realm Realm --
GoogleKeyManagementServiceSecretStore GoogleKeyManagementServiceSecretStore --id id --body body
```

Parameters:

--GoogleKeyManagementServiceSecretStore

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "secretId" : {
      "title" : "Secret ID",
      "description" : "The secret ID that is to be associated with an alias.",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "aliases" : {
      "title" : "Key Name",
      "description" : "The name of the KMS key to use for this purpose. The key must exist in the
 configured key ring.",
      "propertyOrder" : 200,
      "required" : true,
      "items" : {
        "type" : "string",
        "minLength" : 1
      },
      "minItems" : 1,
      "uniqueItems" : true,
      "type" : "array",
      "exampleValue" : ""
    }
  }
}
```

delete

Usage:

```
am> delete GoogleKmsMappings --realm Realm --
GoogleKeyManagementServiceSecretStore GoogleKeyManagementServiceSecretStore --id id
```

Parameters:

--GoogleKeyManagementServiceSecretStore

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action GoogleKmsMappings --realm Realm --
GoogleKeyManagementServiceSecretStore GoogleKeyManagementServiceSecretStore --actionName getAllTypes
```

Parameters:

--GoogleKeyManagementServiceSecretStore

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action GoogleKmsMappings --realm Realm --
GoogleKeyManagementServiceSecretStore GoogleKeyManagementServiceSecretStore --actionName getCreatableTypes
```

Parameters:

--GoogleKeyManagementServiceSecretStore

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action GoogleKmsMappings --realm Realm --
GoogleKeyManagementServiceSecretStore GoogleKeyManagementServiceSecretStore --actionName nextdescendents
```

Parameters:

--GoogleKeyManagementServiceSecretStore

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query GoogleKmsMappings --realm Realm --filter filter --
GoogleKeyManagementServiceSecretStore GoogleKeyManagementServiceSecretStore
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

--GoogleKeyManagementServiceSecretStore

read

Usage:

```
am> read GoogleKmsMappings --realm Realm --
GoogleKeyManagementServiceSecretStore GoogleKeyManagementServiceSecretStore --id id
```

Parameters:

--GoogleKeyManagementServiceSecretStore

--id

The unique identifier for the resource.

update

Usage:

```
am> update GoogleKmsMappings --realm Realm --
GoogleKeyManagementServiceSecretStore GoogleKeyManagementServiceSecretStore --id id --body body
```

Parameters:

--GoogleKeyManagementServiceSecretStore

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "secretId" : {
      "title" : "Secret ID",
      "description" : "The secret ID that is to be associated with an alias.",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "aliases" : {
      "title" : "Key Name",
      "description" : "The name of the KMS key to use for this purpose. The key must exist in the
 configured key ring.",
      "propertyOrder" : 200,
      "required" : true,
      "items" : {
        "type" : "string",
        "minLength" : 1
      },
      "minItems" : 1,
      "uniqueItems" : true,
      "type" : "array",
      "exampleValue" : ""
    }
  }
}
```

Global Operations

Resource path: `/global-config/secrets/stores/GoogleKeyManagementServiceSecretStore/{GoogleKeyManagementServiceSecretStore}/mappings`

Resource version: `1.0`

create

Usage:

```
am> create GoogleKmsMappings --global --
GoogleKeyManagementServiceSecretStore GoogleKeyManagementServiceSecretStore --id id --body body
```

Parameters:

--GoogleKeyManagementServiceSecretStore

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "aliases" : {
      "title" : "Key Name",
      "description" : "The name of the KMS key to use for this purpose. The key must exist in the
 configured key ring.",
      "propertyOrder" : 200,
      "required" : true,
      "items" : {
        "type" : "string",
        "minLength" : 1
      },
      "minItems" : 1,
      "uniqueItems" : true,
      "type" : "array",
      "exampleValue" : ""
    },
    "secretId" : {
      "title" : "Secret ID",
      "description" : "The secret ID that is to be associated with an alias.",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
```

delete

Usage:

```
am> delete GoogleKmsMappings --global --
GoogleKeyManagementServiceSecretStore GoogleKeyManagementServiceSecretStore --id id
```

Parameters:

--GoogleKeyManagementServiceSecretStore

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action GoogleKmsMappings --global --
GoogleKeyManagementServiceSecretStore GoogleKeyManagementServiceSecretStore --actionName getAllTypes
```

Parameters:

--GoogleKeyManagementServiceSecretStore

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action GoogleKmsMappings --global --
GoogleKeyManagementServiceSecretStore GoogleKeyManagementServiceSecretStore --actionName getCreatableTypes
```

Parameters:

--GoogleKeyManagementServiceSecretStore

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action GoogleKmsMappings --global --
GoogleKeyManagementServiceSecretStore GoogleKeyManagementServiceSecretStore --actionName nextdescendents
```

Parameters:

--GoogleKeyManagementServiceSecretStore

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query GoogleKmsMappings --global --filter filter --
GoogleKeyManagementServiceSecretStore GoogleKeyManagementServiceSecretStore
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

--GoogleKeyManagementServiceSecretStore

read

Usage:

```
am> read GoogleKmsMappings --global --
GoogleKeyManagementServiceSecretStore GoogleKeyManagementServiceSecretStore --id id
```

Parameters:

--GoogleKeyManagementServiceSecretStore

--id

The unique identifier for the resource.

update

Usage:

```
am> update GoogleKmsMappings --global --
GoogleKeyManagementServiceSecretStore GoogleKeyManagementServiceSecretStore --id id --body body
```

Parameters:

--GoogleKeyManagementServiceSecretStore

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "aliases" : {
      "title" : "Key Name",
      "description" : "The name of the KMS key to use for this purpose. The key must exist in the
 configured key ring.",
      "propertyOrder" : 200,
      "required" : true,
      "items" : {
        "type" : "string",
        "minLength" : 1
      },
      "minItems" : 1,
      "uniqueItems" : true,
      "type" : "array",
      "exampleValue" : ""
    },
    "secretId" : {
      "title" : "Secret ID",
      "description" : "The secret ID that is to be associated with an alias.",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
```

GraphiteReporter

Global Operations

Resource path: `/global-config/services/monitoring/graphite`

Resource version: `1.0`

create

Usage:

```
am> create GraphiteReporter --global --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "port" : {
      "title" : "Port",
      "description" : "The port of the Graphite server to which metrics should be published.",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "frequency" : {
      "title" : "Frequency",
      "description" : "The frequency (in seconds) at which metrics should be published.",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "host" : {
      "title" : "Hostname",
      "description" : "The hostname of the Graphite server to which metrics should be published.",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
```

delete

Usage:

```
am> delete GraphiteReporter --global --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action GraphiteReporter --global --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action GraphiteReporter --global --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action GraphiteReporter --global --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query GraphiteReporter --global --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read GraphiteReporter --global --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update GraphiteReporter --global --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "port" : {
      "title" : "Port",
      "description" : "The port of the Graphite server to which metrics should be published.",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "frequency" : {
      "title" : "Frequency",
      "description" : "The frequency (in seconds) at which metrics should be published.",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "host" : {
      "title" : "Hostname",
      "description" : "The hostname of the Graphite server to which metrics should be published.",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
```

HOTPGenerator

Realm Operations

Resource path: `/realm-config/authentication/authenticationtrees/nodes/OneTimePasswordGeneratorNode`

Resource version: `1.0`

create

Usage:

```
am> create HOTPGenerator --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "length" : {
      "title" : "One Time Password Length",
      "description" : "The length in characters of the one time password.",
      "propertyOrder" : 100,
      "type" : "integer",
      "exampleValue" : ""
    }
  },
  "required" : [ "length" ]
}
```

delete

Usage:

```
am> delete HOTPGenerator --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action HOTPGenerator --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action HOTPGenerator --realm Realm --actionName getCreatableTypes
```

listOutcomes

List the available outcomes for the node type.

Usage:

```
am> action HOTPGenerator --realm Realm --body body --actionName listOutcomes
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "title" : "Some configuration of the node. This does not need to be complete against the
 configuration schema."
}
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action HOTPGenerator --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query HOTPGenerator --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read HOTPGenerator --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update HOTPGenerator --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "length" : {
      "title" : "One Time Password Length",
      "description" : "The length in characters of the one time password.",
      "propertyOrder" : 100,
      "type" : "integer",
      "exampleValue" : ""
    }
  },
  "required" : [ "length" ]
}
```

HostedSaml2EntityProvider

Realm Operations

Allows the management of hosted SAML2 entity providers.

Resource path: `/realm-config/saml2/hosted`

Resource version: `1.0`

create

create.description

Usage:

```
am> create HostedSaml2EntityProvider --realm Realm --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "$schema" : "http://json-schema.org/draft-07/schema#",
  "ignoredProperties" : [ "_id", "_rev" ],
  "description" : "This schema describes a hosted SAML2 entity provider.",
  "title" : "SAML2 Hosted Entity Provider",
  "type" : "object",
  "properties" : {
    "entityId" : {
      "type" : "string"
    },
    "identityProvider" : {
      "title" : "Identity Provider",
      "description" : "This schema describes a SAML2 identity provider.",
      "type" : "object",
      "traverseObject" : true,
      "properties" : {
        "assertionContent" : {
          "propertyOrder" : 0,
          "title" : "Assertion Content",
          "type" : "object",
          "traverseObject" : true,
          "properties" : {
            "signingAndEncryption" : {
              "traverseObject" : true,
              "title" : "Signing And Encryption",
              "type" : "object",
              "properties" : {
                "requestResponseSigning" : {
                  "traverseObject" : true,
                  "title" : "Request/Response Signing",
                  "description" : "Select the checkbox for each request/response that should be
 signed",
                  "type" : "object",
                  "properties" : {
                    "authenticationRequest" : {
                      "attributePath" : {
                        "value" : "/wantAuthnRequestsSigned"
                      },
                      "title" : "Authentication Request",
                      "type" : "boolean",
                      "default" : false
                    },
                    "artifactResolve" : {
                      "attributeKey" : "wantArtifactResolveSigned",
                      "title" : "Artifact Resolve",
                      "type" : "boolean",
                      "default" : false
                    },
                    "logoutRequest" : {
                      "attributeKey" : "wantLogoutRequestSigned",
                      "title" : "Logout Request",
                      "type" : "boolean",
                      "default" : false
                    },
                    "logoutResponse" : {
```

```
                    "attributeKey" : "wantLogoutResponseSigned",
                    "title" : "Logout Response",
                    "type" : "boolean",
                    "default" : false
                  },
                  "manageNameIdRequest" : {
                    "attributeKey" : "wantMNIRequestSigned",
                    "title" : "Manage NameID Request",
                    "type" : "boolean",
                    "default" : false
                  },
                  "manageNameIdResponse" : {
                    "attributeKey" : "wantMNIResponseSigned",
                    "title" : "Manage NameID Response",
                    "type" : "boolean",
                    "default" : false
                  }
                },
                "required" : [ "authenticationRequest", "artifactResolve", "logoutRequest",
"logoutResponse", "manageNameIdRequest", "manageNameIdResponse" ]
              },
              "encryption" : {
                "traverseObject" : true,
                "title" : "Encryption",
                "type" : "object",
                "properties" : {
                  "nameIdEncryption" : {
                    "attributeKey" : "wantNameIDEncrypted",
                    "title" : "NameID Encryption",
                    "type" : "boolean",
                    "default" : false
                  }
                },
                "required" : [ "nameIdEncryption" ]
              },
              "secretIdAndAlgorithms" : {
                "traverseObject" : true,
                "title" : "Secret ID And Algorithms",
                "type" : "object",
                "properties" : {
                  "secretIdIdentifier" : {
                    "type" : "string",
                    "attributeKey" : "secretIdIdentifier",
                    "title" : "Secret ID Identifier",
                    "description" : "This identifier determines the secret ID for this
entity provider when resolving secrets. For example when this value is set to \"demo\", the
entity provider will use am.applications.federation.entity.providers.saml2.demo.signing and
am.applications.federation.entity.providers.saml2.demo.encryption secret IDs to resolve the signing
and encryption secrets. When left unspecified, AM will use the entity provider role (service
provider, identity provider, etc.) specific default global secret IDs. When the secret ID identifier
for a given role is modified, the corresponding mapping is removed if it isnâ##t referenced by other
entities."
                  },
                  "signingAlgorithm" : {
                    "title" : "Signing Algorithm",
                    "type" : "array",
                    "attributePath" : {
                      "value" : "extensions",
```

```
                        "mapper" :
 "org.forgerock.openam.federation.rest.schema.mappers.SigningAlgorithmMapper"
                      },
                      "items" : {
                        "type" : "string",
                        "enum" : [ "http://www.w3.org/2000/09/xmldsig#rsa-sha1", "http://
www.w3.org/2001/04/xmldsig-more#ecdsa-sha256", "http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha384",
 "http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha512", "http://www.w3.org/2001/04/xmldsig-more#rsa-
sha256", "http://www.w3.org/2001/04/xmldsig-more#rsa-sha384", "http://www.w3.org/2001/04/xmldsig-
more#rsa-sha512", "http://www.w3.org/2009/xmldsig11#dsa-sha256" ],
                        "enumNames" : [ "http://www.w3.org/2000/09/xmldsig#rsa-sha1", "http://
www.w3.org/2001/04/xmldsig-more#ecdsa-sha256", "http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha384",
 "http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha512", "http://www.w3.org/2001/04/xmldsig-more#rsa-
sha256", "http://www.w3.org/2001/04/xmldsig-more#rsa-sha384", "http://www.w3.org/2001/04/xmldsig-
more#rsa-sha512", "http://www.w3.org/2009/xmldsig11#dsa-sha256" ]
                      }
                    },
                    "digestAlgorithm" : {
                      "title" : "Digest Algorithm",
                      "type" : "array",
                      "attributePath" : {
                        "value" : "extensions",
                        "mapper" :
 "org.forgerock.openam.federation.rest.schema.mappers.DigestAlgorithmMapper"
                      },
                      "items" : {
                        "type" : "string",
                        "enum" : [ "http://www.w3.org/2000/09/xmldsig#sha1", "http://
www.w3.org/2001/04/xmldsig-more#sha384", "http://www.w3.org/2001/04/xmlenc#sha256", "http://
www.w3.org/2001/04/xmlenc#sha512", "http://www.w3.org/2007/05/xmldsig-more#sha3-256", "http://
www.w3.org/2007/05/xmldsig-more#sha3-384", "http://www.w3.org/2007/05/xmldsig-more#sha3-512" ],
                        "enumNames" : [ "http://www.w3.org/2000/09/xmldsig#sha1", "http://
www.w3.org/2001/04/xmldsig-more#sha384", "http://www.w3.org/2001/04/xmlenc#sha256", "http://
www.w3.org/2001/04/xmlenc#sha512", "http://www.w3.org/2007/05/xmldsig-more#sha3-256", "http://
www.w3.org/2007/05/xmldsig-more#sha3-384", "http://www.w3.org/2007/05/xmldsig-more#sha3-512" ]
                      }
                    },
                    "encryptionAlgorithm" : {
                      "title" : "Encryption Algorithm",
                      "type" : "array",
                      "attributeKey" : {
                        "value" : "encryptionAlgorithms",
                        "mapper" :
 "org.forgerock.openam.federation.rest.schema.mappers.EncryptionAlgorithmMapper"
                      },
                      "items" : {
                        "type" : "string",
                        "enum" : [ "http://www.w3.org/2009/xmlenc11#aes128-gcm", "http://
www.w3.org/2009/xmlenc11#aes192-gcm", "http://www.w3.org/2009/xmlenc11#aes256-gcm", "http://
www.w3.org/2001/04/xmlenc#aes128-cbc", "http://www.w3.org/2001/04/xmlenc#aes192-cbc", "http://
www.w3.org/2001/04/xmlenc#aes256-cbc", "http://www.w3.org/2001/04/xmlenc#rsa-1_5", "http://
www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p", "http://www.w3.org/2009/xmlenc11#rsa-oaep" ],
                        "enumNames" : [ "http://www.w3.org/2009/xmlenc11#aes128-gcm", "http://
www.w3.org/2009/xmlenc11#aes192-gcm", "http://www.w3.org/2009/xmlenc11#aes256-gcm", "http://
www.w3.org/2001/04/xmlenc#aes128-cbc", "http://www.w3.org/2001/04/xmlenc#aes192-cbc", "http://
www.w3.org/2001/04/xmlenc#aes256-cbc", "http://www.w3.org/2001/04/xmlenc#rsa-1_5", "http://
www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p", "http://www.w3.org/2009/xmlenc11#rsa-oaep" ]
                      }
                    }
```

```
                }
              }
            }
          },
          "nameIdFormat" : {
            "traverseObject" : true,
            "title" : "NameID Format",
            "type" : "object",
            "properties" : {
              "nameIdFormatList" : {
                "description" : "List of NameID formats the requestor will use to contact. Order
 listed shows the order of preference",
                "title" : "NameID Format List",
                "attributePath" : {
                  "value" : "/nameIDFormat"
                },
                "type" : "array",
                "items" : {
                  "type" : "string"
                },
                "default" : [ "urn:oasis:names:tc:SAML:2.0:nameid-format:persistent",
 "urn:oasis:names:tc:SAML:2.0:nameid-format:transient", "urn:oasis:names:tc:SAML:1.1:nameid-
format:emailAddress", "urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified",
 "urn:oasis:names:tc:SAML:1.1:nameid-format:WindowsDomainQualifiedName",
 "urn:oasis:names:tc:SAML:2.0:nameid-format:kerberos", "urn:oasis:names:tc:SAML:1.1:nameid-
format:X509SubjectName" ]
              },
              "nameIdValueMap" : {
                "attributeKey" : {
                  "value" : "nameIDFormatMap",
                  "mapper" : "org.forgerock.openam.federation.rest.schema.mappers.NameIdValueMapper"
                },
                "description" : "Defines mapping between the NameID format and user's profile
 attribute. Example <code>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress=mail</code> or
 <code>urn:oasis:names:tc:SAML:2.0:nameid-format:persistent=objectGUID;binary</code>. If the defined
 NameID format is used in protocol, the profile attribute value will be used as NameID value for
 the format in the Subject, the <code>;binary</code> flag can be used to indicate that the profile
 attribute is binary and should be Base64 encoded when used as the NameID value.",
                "title" : "NameID Value Map",
                "type" : "array",
                "items" : {
                  "type" : "object",
                  "properties" : {
                    "key" : {
                      "title" : "Key",
                      "propertyOrder" : 0,
                      "type" : "string"
                    },
                    "value" : {
                      "title" : "Value",
                      "propertyOrder" : 1,
                      "type" : "string"
                    },
                    "binary" : {
                      "title" : "Binary",
                      "propertyOrder" : 2,
                      "type" : "boolean"
                    }
                  }
```

```
                },
                "default" : [ {
                  "key" : "urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress",
                  "value" : "mail",
                  "binary" : false
                } ]
              }
            }
          },
          "authenticationContext" : {
            "title" : "Authentication Context",
            "type" : "object",
            "traverseObject" : true,
            "properties" : {
              "authenticationContextMapper" : {
                "attributeKey" : "idpAuthncontextMapper",
                "title" : "Mapper",
                "type" : "string",
                "default" : "com.sun.identity.saml2.plugins.DefaultIDPAuthnContextMapper"
              },
              "authContextItems" : {
                "title" : "Authentication Context",
                "description" : "Defines mapping between SP requested Authentication Context
Reference and IDP authentication scheme and authentication level.",
                "type" : "array",
                "attributeKey" : {
                  "value" : "idpAuthncontextClassrefMapping",
                  "mapper" :
"org.forgerock.openam.federation.rest.schema.mappers.IdpAuthContextMapper"
                },
                "items" : {
                  "type" : "object",
                  "properties" : {
                    "contextReference" : {
                      "propertyOrder" : 0,
                      "title" : "Context Reference",
                      "anyOf" : [ {
                        "title" : "Predefined Reference",
                        "type" : "string",
                        "enum" : [ "urn:oasis:names:tc:SAML:2.0:ac:classes:InternetProtocol",
"urn:oasis:names:tc:SAML:2.0:ac:classes:InternetProtocolPassword",
"urn:oasis:names:tc:SAML:2.0:ac:classes:Kerberos",
"urn:oasis:names:tc:SAML:2.0:ac:classes:MobileOneFactorUnregistered",
"urn:oasis:names:tc:SAML:2.0:ac:classes:MobileTwoFactorUnregistered",
"urn:oasis:names:tc:SAML:2.0:ac:classes:MobileOneFactorContract",
"urn:oasis:names:tc:SAML:2.0:ac:classes:MobileTwoFactorContract",
"urn:oasis:names:tc:SAML:2.0:ac:classes:Password",
"urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport",
"urn:oasis:names:tc:SAML:2.0:ac:classes:PreviousSession",
"urn:oasis:names:tc:SAML:2.0:ac:classes:X.509", "urn:oasis:names:tc:SAML:2.0:ac:classes:PGP",
"urn:oasis:names:tc:SAML:2.0:ac:classes:SPKI", "urn:oasis:names:tc:SAML:2.0:ac:classes:XMLDSig",
"urn:oasis:names:tc:SAML:2.0:ac:classes:Smartcard",
"urn:oasis:names:tc:SAML:2.0:ac:classes:SmartcardPKI",
"urn:oasis:names:tc:SAML:2.0:ac:classes:SoftwarePKI",
"urn:oasis:names:tc:SAML:2.0:ac:classes:Telephony",
"urn:oasis:names:tc:SAML:2.0:ac:classes:NomadTelephony",
"urn:oasis:names:tc:SAML:2.0:ac:classes:PersonalTelephony",
"urn:oasis:names:tc:SAML:2.0:ac:classes:AuthenticatedTelephony",
"urn:oasis:names:tc:SAML:2.0:ac:classes:SecureRemotePassword",
```

```
"urn:oasis:names:tc:SAML:2.0:ac:classes:TLSClient",
"urn:oasis:names:tc:SAML:2.0:ac:classes:TimeSyncToken", "unspecified" ],
                        "enumNames" : [ "InternetProtocol", "InternetProtocolPassword", "Kerberos",
"MobileOneFactorUnregistered", "MobileTwoFactorUnregistered", "MobileOneFactorContract",
"MobileTwoFactorContract", "Password", "PasswordProtectedTransport", "PreviousSession", "X.509",
"PGP", "SPKI", "XMLDSig", "Smartcard", "SmartcardPKI", "SoftwarePKI", "Telephony", "NomadTelephony",
"PersonalTelephony", "AuthenticatedTelephony", "SecureRemotePassword", "TLSClient", "TimeSyncToken",
"unspecified" ]
                      }, {
                        "title" : "Custom Reference",
                        "type" : "string"
                      } ]
                    },
                    "key" : {
                      "propertyOrder" : 1,
                      "type" : "string",
                      "title" : "Key",
                      "enum" : [ "service", "module", "user", "role", "authlevel" ],
                      "enumNames" : [ "Service", "Module", "User", "Role", "Authentication Level" ]
                    },
                    "value" : {
                      "propertyOrder" : 2,
                      "title" : "Value",
                      "type" : "string"
                    },
                    "level" : {
                      "propertyOrder" : 3,
                      "title" : "Level",
                      "type" : "integer",
                      "minimum" : 0
                    }
                  }
                },
                "default" : [ {
                  "contextReference" :
"urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport",
                  "level" : "0"
                } ]
              }
            }
          },
          "assertionTime" : {
            "traverseObject" : true,
            "title" : "Assertion Time",
            "type" : "object",
            "properties" : {
              "notBeforeTimeSkew" : {
                "attributeKey" : "assertionNotBeforeTimeSkew",
                "title" : "Not-Before Time Skew",
                "type" : "integer",
                "minimum" : 0,
                "default" : 600,
                "description" : "Is in seconds. This is the skew time for NotBefore attributes in
assertion"
              },
              "effectiveTime" : {
                "attributeKey" : "assertionEffectiveTime",
                "title" : "Effective Time",
                "type" : "integer",
```

```
                "minimum" : 0,
                "description" : "Is in seconds. Validity time of assertion for NotAfter attributes",
                "default" : 600
              }
            }
          },
          "basicAuthentication" : {
            "traverseObject" : true,
            "description" : "Configure basic authentication setting for Soap based binding",
            "title" : "Basic Authentication",
            "type" : "object",
            "properties" : {
              "enabled" : {
                "attributeKey" : "basicAuthOn",
                "title" : "Enabled",
                "type" : "boolean",
                "default" : false
              },
              "userName" : {
                "attributeKey" : "basicAuthUser",
                "title" : "User Name",
                "type" : "string"
              },
              "password" : {
                "title" : "Password",
                "attributeKey" : {
                  "value" : "basicAuthPassword",
                  "mapper" : "org.forgerock.openam.federation.rest.schema.mappers.PasswordMapper"
                },
                "type" : "string",
                "format" : "password"
              }
            }
          },
          "assertionCache" : {
            "traverseObject" : true,
            "type" : "object",
            "title" : "Assertion Cache",
            "properties" : {
              "enabled" : {
                "attributeKey" : "assertionCacheEnabled",
                "description" : "Enable assertion cache",
                "title" : "Enabled",
                "type" : "boolean",
                "default" : false
              }
            }
          }
        }
      },
      "assertionProcessing" : {
        "propertyOrder" : 1,
        "title" : "Assertion Processing",
        "type" : "object",
        "traverseObject" : true,
        "properties" : {
          "attributeMapper" : {
            "title" : "Attribute Mapper",
            "type" : "object",
```

```
              "traverseObject" : true,
              "properties" : {
                "attributeMapper" : {
                  "attributeKey" : "idpAttributeMapper",
                  "title" : "Attribute Mapper",
                  "type" : "string",
                  "default" : "com.sun.identity.saml2.plugins.DefaultIDPAttributeMapper"
                },
                "attributeMap" : {
                  "title" : "Attribute Map",
                  "description" : "This mapping is the configuration used by the Attribute Mapper.
 The mapping should be defined as [NameFormatURI|]SAML ATTRIBUTE NAME=PROFILE ATTRIBUTE NAME in
 assertion. Example: EmailAddress=mail, Address=postaladdress, urn:oasis:names:tc:SAML:2.0:attrname-
format:uri|urn:mace:dir:attribute-def:cn=cn The mapper also allows for static values to be defined.
 To define a static value, enclose the profile attribute name in double quotes. Example: partnerID=
\"staticPartnerIDValue\", urn:oasis:names:tc:SAML:2.0:attrname-format:uri|nameID=\"staticNameIDValue
\". To flag an attribute as being a binary value and have its value Base64 encoded, add ;binary to the
 end of the profile attribute name. Example: photo=photo;binary, urn:oasis:names:tc:SAML:2.0:attrname-
format:uri|photo=photo;binary",
                  "type" : "array",
                  "attributeKey" : {
                    "value" : "attributeMap",
                    "mapper" :
 "org.forgerock.openam.federation.rest.schema.mappers.AttributeMapMapper"
                  },
                  "items" : {
                    "type" : "object",
                    "properties" : {
                      "nameFormatUri" : {
                        "title" : "Name Format Uri",
                        "propertyOrder" : 0,
                        "type" : "string"
                      },
                      "samlAttribute" : {
                        "title" : "SAML Attribute",
                        "propertyOrder" : 1,
                        "type" : "string"
                      },
                      "localAttribute" : {
                        "title" : "Local Attribute",
                        "propertyOrder" : 2,
                        "type" : "string"
                      },
                      "binary" : {
                        "title" : "Binary",
                        "propertyOrder" : 3,
                        "type" : "boolean"
                      }
                    },
                    "required" : [ "samlAttribute", "localAttribute" ]
                  }
                }
              },
              "required" : [ "attributeMapper" ]
            },
            "accountMapper" : {
              "traverseObject" : true,
              "title" : "Account Mapper",
              "type" : "object",
```

```
              "properties" : {
                "accountMapper" : {
                  "attributeKey" : "idpAccountMapper",
                  "title" : "Account Mapper",
                  "type" : "string",
                  "default" : "com.sun.identity.saml2.plugins.DefaultIDPAccountMapper",
                  "description" : "Used to generate Name Identifier in Single Sign-on assertion and
find user's identity from incoming request."
                },
                "disableNameIdPersistence" : {
                  "attributeKey" : "idpDisableNameIDPersistence",
                  "title" : "Disable NameID Persistence",
                  "type" : "boolean",
                  "description" : "Disables the persistence of the NameID values into the User Data
Store for all persistent NameID-Formats. When the persistent NameID-Format is in use, disabling
NameID persistence is not recommended. Note that by preventing the storage of the NameID values,
the ManageNameID and the NameIDMapping SAML profiles will no longer work when using any persistent
NameID-Formats. Existing account links that have been established (and persisted) previously, will
not be removed when enabling this feature.",
                  "default" : false
                }
              }
            },
            "localConfiguration" : {
              "traverseObject" : true,
              "title" : "Local Configuration",
              "type" : "object",
              "properties" : {
                "authUrl" : {
                  "attributeKey" : "AuthUrl",
                  "type" : "string",
                  "title" : "Auth URL",
                  "description" : "URL to redirect for user authentication if required"
                },
                "reverseProxyUrl" : {
                  "attributeKey" : "RpUrl",
                  "type" : "string",
                  "title" : "Reverse Proxy URL",
                  "description" : "URL of the Reverse Proxy where the SAML endpoints are available"
                },
                "externalApplicationLogoutUrl" : {
                  "attributeKey" : "appLogoutUrl",
                  "type" : "string",
                  "title" : "External Application Logout URL",
                  "description" : "This is the logout URL for an external application. Once the server
receives logout request from the remote partner, a request will be sent to the logout URL using back
channel HTTP POST with all cookies. Optionally, a user session property could be sent as HTTP header
and POST parameter if a query parameter \"appsessionproperty\" (set to the session property name) is
included in the URL. e.g. \"http://www.app.domain.com/uri/logout?appsessionproperty=mail\"."
                }
              }
            }
          }
        },
        "services" : {
          "propertyOrder" : 2,
          "title" : "Services",
          "type" : "object",
          "traverseObject" : true,
```

```
          "properties" : {
            "metaAlias" : {
              "attributeKey" : "metaAlias",
              "default" : "{idpMetaAlias}",
              "type" : "string",
              "title" : "Meta Alias",
              "readOnly" : true,
              "description" : "The Meta Alias attribute is specific to providers using OpenAM
therefore, a null value for a remote provider configuration is possible."
            },
            "serviceAttributes" : {
              "title" : "IDP Service Attributes",
              "type" : "object",
              "traverseObject" : true,
              "properties" : {
                "artifactResolutionService" : {
                  "title" : "Artifact Resolution Service",
                  "type" : "array",
                  "attributePath" : {
                    "value" : "artifactResolutionService",
                    "mapper" :
"org.forgerock.openam.federation.rest.schema.mappers.IndexedEndpointMapper"
                  },
                  "items" : {
                    "type" : "object",
                    "properties" : {
                      "binding" : {
                        "title" : "Binding",
                        "anyOf" : [ {
                          "title" : "Predefined Binding",
                          "type" : "string",
                          "enum" : [ "urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect",
"urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST", "urn:oasis:names:tc:SAML:2.0:bindings:SOAP",
"urn:oasis:names:tc:SAML:2.0:bindings:PAOS" ],
                          "enumNames" : [ "HTTP-REDIRECT", "HTTP-POST", "SOAP", "PAOS" ]
                        }, {
                          "title" : "Custom Binding",
                          "type" : "string"
                        } ]
                      },
                      "location" : {
                        "title" : "Location",
                        "type" : "string"
                      },
                      "responseLocation" : {
                        "title" : "Response Location",
                        "type" : "string"
                      }
                    },
                    "required" : [ "location" ]
                  },
                  "default" : [ {
                    "binding" : "urn:oasis:names:tc:SAML:2.0:bindings:SOAP",
                    "location" : "{baseUrl}/ArtifactResolver/metaAlias{idpMetaAlias}"
                  } ]
                },
                "singleLogoutService" : {
                  "title" : "Single Logout Service",
                  "type" : "array",
```

```
                "attributePath" : {
                  "value" : "singleLogoutService",
                  "mapper" : "org.forgerock.openam.federation.rest.schema.mappers.EndpointMapper"
                },
                "items" : {
                  "type" : "object",
                  "properties" : {
                    "binding" : {
                      "title" : "Binding",
                      "anyOf" : [ {
                        "title" : "Predefined Binding",
                        "type" : "string",
                        "enum" : [ "urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect",
"urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST", "urn:oasis:names:tc:SAML:2.0:bindings:SOAP",
"urn:oasis:names:tc:SAML:2.0:bindings:PAOS" ],
                        "enumNames" : [ "HTTP-REDIRECT", "HTTP-POST", "SOAP", "PAOS" ]
                      }, {
                        "title" : "Custom Binding",
                        "type" : "string"
                      } ]
                    },
                    "location" : {
                      "title" : "Location",
                      "type" : "string"
                    },
                    "responseLocation" : {
                      "title" : "Response Location",
                      "type" : "string"
                    }
                  },
                  "required" : [ "location" ]
                },
                "default" : [ {
                  "binding" : "urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect",
                  "location" : "{baseUrl}/IDPSloRedirect/metaAlias{idpMetaAlias}",
                  "responseLocation" : "{baseUrl}/IDPSloRedirect/metaAlias{idpMetaAlias}"
                }, {
                  "binding" : "urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST",
                  "location" : "{baseUrl}/IDPSloPOST/metaAlias{idpMetaAlias}",
                  "responseLocation" : "{baseUrl}/IDPSloPOST/metaAlias{idpMetaAlias}"
                }, {
                  "binding" : "urn:oasis:names:tc:SAML:2.0:bindings:SOAP",
                  "location" : "{baseUrl}/IDPSloSoap/metaAlias{idpMetaAlias}"
                } ]
              },
              "nameIdService" : {
                "title" : "Manage NameID Service",
                "type" : "array",
                "attributePath" : {
                  "value" : "manageNameIDService",
                  "mapper" : "org.forgerock.openam.federation.rest.schema.mappers.EndpointMapper"
                },
                "items" : {
                  "type" : "object",
                  "properties" : {
                    "binding" : {
                      "title" : "Binding",
                      "anyOf" : [ {
                        "title" : "Predefined Binding",
```

```
                        "type" : "string",
                        "enum" : [ "urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect",
"urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST", "urn:oasis:names:tc:SAML:2.0:bindings:SOAP",
"urn:oasis:names:tc:SAML:2.0:bindings:PAOS" ],
                        "enumNames" : [ "HTTP-REDIRECT", "HTTP-POST", "SOAP", "PAOS" ]
                      }, {
                        "title" : "Custom Binding",
                        "type" : "string"
                      } ]
                    },
                    "location" : {
                      "title" : "Location",
                      "type" : "string"
                    },
                    "responseLocation" : {
                      "title" : "Response Location",
                      "type" : "string"
                    }
                  },
                  "required" : [ "location" ]
                },
                "default" : [ {
                  "binding" : "urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect",
                  "location" : "{baseUrl}/IDPMniRedirect/metaAlias{idpMetaAlias}",
                  "responseLocation" : "{baseUrl}/IDPMniRedirect/metaAlias{idpMetaAlias}"
                }, {
                  "binding" : "urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST",
                  "location" : "{baseUrl}/IDPMniPOST/metaAlias{idpMetaAlias}",
                  "responseLocation" : "{baseUrl}/IDPMniPOST/metaAlias{idpMetaAlias}"
                }, {
                  "binding" : "urn:oasis:names:tc:SAML:2.0:bindings:SOAP",
                  "location" : "{baseUrl}/IDPMniSoap/metaAlias{idpMetaAlias}"
                } ]
              },
              "singleSignOnService" : {
                "title" : "Single SignOn Service",
                "type" : "array",
                "attributePath" : {
                  "value" : "singleSignOnService",
                  "mapper" : "org.forgerock.openam.federation.rest.schema.mappers.EndpointMapper"
                },
                "items" : {
                  "type" : "object",
                  "properties" : {
                    "binding" : {
                      "title" : "Binding",
                      "anyOf" : [ {
                        "title" : "Predefined Binding",
                        "type" : "string",
                        "enum" : [ "urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect",
"urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST", "urn:oasis:names:tc:SAML:2.0:bindings:SOAP",
"urn:oasis:names:tc:SAML:2.0:bindings:PAOS" ],
                        "enumNames" : [ "HTTP-REDIRECT", "HTTP-POST", "SOAP", "PAOS" ]
                      }, {
                        "title" : "Custom Binding",
                        "type" : "string"
                      } ]
                    },
                    "location" : {
```

```
                        "title" : "Location",
                        "type" : "string"
                      },
                      "responseLocation" : {
                        "title" : "Response Location",
                        "type" : "string"
                      }
                    },
                    "required" : [ "location" ]
                  },
                  "default" : [ {
                    "binding" : "urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect",
                    "location" : "{baseUrl}/SSORedirect/metaAlias{idpMetaAlias}"
                  }, {
                    "binding" : "urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST",
                    "location" : "{baseUrl}/SSOPOST/metaAlias{idpMetaAlias}"
                  }, {
                    "binding" : "urn:oasis:names:tc:SAML:2.0:bindings:SOAP",
                    "location" : "{baseUrl}/SSOSoap/metaAlias{idpMetaAlias}"
                  } ]
                }
              }
            },
            "nameIdMapping" : {
              "title" : "NameID Mapping",
              "type" : "array",
              "attributePath" : {
                "value" : "nameIDMappingService",
                "mapper" : "org.forgerock.openam.federation.rest.schema.mappers.EndpointMapper"
              },
              "items" : {
                "type" : "object",
                "properties" : {
                  "binding" : {
                    "title" : "Binding",
                    "anyOf" : [ {
                      "title" : "Predefined Binding",
                      "type" : "string",
                      "enum" : [ "urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect",
"urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST", "urn:oasis:names:tc:SAML:2.0:bindings:SOAP",
"urn:oasis:names:tc:SAML:2.0:bindings:PAOS" ],
                      "enumNames" : [ "HTTP-REDIRECT", "HTTP-POST", "SOAP", "PAOS" ]
                    }, {
                      "title" : "Custom Binding",
                      "type" : "string"
                    } ]
                  },
                  "location" : {
                    "title" : "Location",
                    "type" : "string"
                  },
                  "responseLocation" : {
                    "title" : "Response Location",
                    "type" : "string"
                  }
                },
                "required" : [ "location" ]
              },
              "default" : [ {
```

```
                "binding" : "urn:oasis:names:tc:SAML:2.0:bindings:SOAP",
                "location" : "{baseUrl}/NIMSoap/metaAlias{idpMetaAlias}"
              } ]
            },
            "assertionIdRequest" : {
              "title" : "Assertion ID Request Service",
              "type" : "array",
              "attributePath" : {
                "value" : "assertionIDRequestService",
                "mapper" : "org.forgerock.openam.federation.rest.schema.mappers.EndpointMapper"
              },
              "items" : {
                "type" : "object",
                "properties" : {
                  "binding" : {
                    "title" : "Binding",
                    "anyOf" : [ {
                      "title" : "Predefined Binding",
                      "type" : "string",
                      "enum" : [ "urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect",
"urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST", "urn:oasis:names:tc:SAML:2.0:bindings:SOAP",
"urn:oasis:names:tc:SAML:2.0:bindings:PAOS" ],
                      "enumNames" : [ "HTTP-REDIRECT", "HTTP-POST", "SOAP", "PAOS" ]
                    }, {
                      "title" : "Custom Binding",
                      "type" : "string"
                    } ]
                  },
                  "location" : {
                    "title" : "Location",
                    "type" : "string"
                  },
                  "responseLocation" : {
                    "title" : "Response Location",
                    "type" : "string"
                  }
                },
                "required" : [ "location" ]
              },
              "default" : [ {
                "binding" : "urn:oasis:names:tc:SAML:2.0:bindings:SOAP",
                "location" : "{baseUrl}/AIDReqSoap/IDPRole/metaAlias{idpMetaAlias}"
              }, {
                "binding" : "urn:oasis:names:tc:SAML:2.0:bindings:URI",
                "location" : "{baseUrl}/AIDReqUri/IDPRole/metaAlias{idpMetaAlias}"
              } ]
            }
          },
          "required" : [ "metaAlias" ]
        },
        "advanced" : {
          "traverseObject" : true,
          "propertyOrder" : 3,
          "title" : "Advanced",
          "type" : "object",
          "properties" : {
            "saeConfiguration" : {
              "traverseObject" : true,
              "title" : "SAE Configuration",
```

```
              "type" : "object",
              "properties" : {
                "idpUrl" : {
                  "attributeKey" : "saeIDPUrl",
                  "title" : "IDP URL",
                  "description" : "URL endpoint on the Identity Provider that can handle SAE
requests.",
                  "type" : "string",
                  "default" : "{baseUrl}/idpsaehandler/metaAlias{idpMetaAlias}"
                },
                "applicationSecurityConfiguration" : {
                  "attributeKey" : {
                    "value" : "saeAppSecretList",
                    "mapper" :
"org.forgerock.openam.federation.rest.schema.mappers.ApplicationSecurityConfigItemMapper"
                  },
                  "title" : "Application Security Configuration",
                  "type" : "array",
                  "items" : {
                    "type" : "object",
                    "properties" : {
                      "url" : {
                        "title" : "URL",
                        "propertyOrder" : 0,
                        "type" : "string"
                      },
                      "type" : {
                        "title" : "Type",
                        "propertyOrder" : 1,
                        "type" : "string"
                      },
                      "pubKeyAlias" : {
                        "title" : "Public Key Alias",
                        "propertyOrder" : 2,
                        "type" : "string"
                      },
                      "encryptionAlgorithm" : {
                        "title" : "Encryption Algorithm",
                        "propertyOrder" : 3,
                        "type" : "string"
                      },
                      "encryptionKeyStrength" : {
                        "title" : "Encryption Key Strength",
                        "propertyOrder" : 4,
                        "type" : "string"
                      },
                      "secret" : {
                        "title" : "Secret",
                        "propertyOrder" : 5,
                        "type" : "string"
                      }
                    },
                    "required" : [ "url", "secret" ]
                  }
                }
              }
            },
            "ecpConfiguration" : {
              "traverseObject" : true,
```

```
              "title" : "ECP Configuration",
              "type" : "object",
              "properties" : {
                "idpSessionMapper" : {
                  "attributeKey" : "idpECPSessionMapper",
                  "title" : "IDP Session Mapper",
                  "description" : "Defines an implementation class for the session mapper SPI. The
mapper finds a valid session from HTTP servlet request on IDP with ECP profile.",
                  "type" : "string",
                  "default" : "com.sun.identity.saml2.plugins.DefaultIDPECPSessionMapper"
                }
              }
            },
            "sessionSynchronization" : {
              "traverseObject" : true,
              "title" : "Session Synchronization",
              "type" : "object",
              "properties" : {
                "enabled" : {
                  "attributeKey" : "idpSessionSyncEnabled",
                  "title" : "Enabled",
                  "description" : "If this is enabled, when a session times out, the Identity Provider
notifies all Service Providers to log out. A session may time out, for example, when max-idle time or
max-session time is reached.",
                  "type" : "boolean",
                  "default" : false
                }
              }
            },
            "idpFinderImplementation" : {
              "traverseObject" : true,
              "title" : "IDP Finder Implementation",
              "type" : "object",
              "properties" : {
                "idpFinderImplementationClass" : {
                  "attributeKey" : "proxyIDPFinderClass",
                  "title" : "IDP Finder implementation class",
                  "description" : "Defines an implementation class for the Proxy IDP Finder SPI. The
implementation is used to find a preferred IdP to send the proxied Authentication Request",
                  "type" : "string"
                },
                "idpFinderJsp" : {
                  "attributeKey" : "proxyIDPFinderJSP",
                  "title" : "IdP Finder JSP",
                  "description" : "Specify the JSP that will present the IdP List to the user, if
required by the class implementation (example: proxyidpfinder.jsp)",
                  "type" : "string"
                },
                "enableProxyIdpFinderForAllSps" : {
                  "attributeKey" : "enableProxyIDPFinderForAllSPs",
                  "title" : "Enable Proxy IDP Finder for all SPs",
                  "description" : "If this is enabled the proxy idp finder will be enabled for all the
remote SPs regardless of what they have configured in their extended metadata",
                  "type" : "boolean",
                  "default" : false
                }
              }
            },
            "relayStateUrlList" : {
```

```
              "traverseObject" : true,
              "title" : "Relay State URL List",
              "type" : "object",
              "properties" : {
                "relayStateUrlList" : {
                  "attributeKey" : "relayStateUrlList",
                  "title" : "Relay State URL List",
                  "type" : "array",
                  "items" : {
                    "type" : "string"
                  }
                }
              }
            },
            "idpAdapter" : {
              "traverseObject" : true,
              "title" : "IDP Adapter",
              "type" : "object",
              "properties" : {
                "idpAdapterClass" : {
                  "attributeKey" : "idpAdapter",
                  "title" : "IDP Adapter Class",
                  "type" : "string"
                }
              }
            }
          }
        }
      }
    },
    "serviceProvider" : {
      "title" : "Service Provider",
      "description" : "This schema describes a SAML2 service provider.",
      "type" : "object",
      "traverseObject" : true,
      "properties" : {
        "assertionContent" : {
          "propertyOrder" : 0,
          "traverseObject" : true,
          "title" : "Assertion Content",
          "type" : "object",
          "properties" : {
            "signingAndEncryption" : {
              "traverseObject" : true,
              "title" : "Signing And Encryption",
              "type" : "object",
              "properties" : {
                "requestResponseSigning" : {
                  "traverseObject" : true,
                  "description" : "Select the checkbox for each request/response that should be signed
\n",
                  "title" : "Request/Response Signing",
                  "type" : "object",
                  "properties" : {
                    "authenticationRequest" : {
                      "attributePath" : {
                        "value" : "/authnRequestsSigned"
                      },
                      "title" : "Authentication Requests Signed",
```

```
                    "type" : "boolean",
                    "default" : false
                  },
                  "assertion" : {
                    "attributePath" : "/wantAssertionsSigned",
                    "title" : "Assertions Signed",
                    "type" : "boolean",
                    "default" : false
                  },
                  "postResponse" : {
                    "attributeKey" : "wantPOSTResponseSigned",
                    "title" : "POST Response Signed",
                    "type" : "boolean",
                    "default" : false
                  },
                  "artifactResponse" : {
                    "attributeKey" : "wantArtifactResponseSigned",
                    "title" : "Artifact Response Signed",
                    "type" : "boolean",
                    "default" : false
                  },
                  "logoutRequest" : {
                    "attributeKey" : "wantLogoutRequestSigned",
                    "title" : "Logout Request Signed",
                    "type" : "boolean",
                    "default" : false
                  },
                  "logoutResponse" : {
                    "attributeKey" : "wantLogoutResponseSigned",
                    "title" : "Logout Response Signed",
                    "type" : "boolean",
                    "default" : false
                  },
                  "manageNameIdRequest" : {
                    "attributeKey" : "wantMNIRequestSigned",
                    "title" : "Manage NameID Request Signed",
                    "type" : "boolean",
                    "default" : false
                  },
                  "manageNameIdResponse" : {
                    "attributeKey" : "wantMNIResponseSigned",
                    "title" : "Manage NameID Response Signed",
                    "type" : "boolean",
                    "default" : false
                  }
                }
              },
              "encryption" : {
                "traverseObject" : true,
                "title" : "Encryption",
                "type" : "object",
                "properties" : {
                  "attributeEncryption" : {
                    "attributeKey" : "wantAttributeEncrypted",
                    "title" : "Attribute Encryption",
                    "type" : "boolean"
                  },
                  "assertionEncryption" : {
                    "attributeKey" : "wantAssertionEncrypted",
```

```
                      "title" : "Assertion Encryption",
                      "type" : "boolean"
                    },
                    "nameIdEncryption" : {
                      "attributeKey" : "wantNameIDEncrypted",
                      "title" : "NameID Encryption",
                      "type" : "boolean"
                    }
                  }
                },
                "secretIdAndAlgorithms" : {
                  "traverseObject" : true,
                  "title" : "Secret ID And Algorithms",
                  "type" : "object",
                  "properties" : {
                    "secretIdIdentifier" : {
                      "type" : "string",
                      "attributeKey" : "secretIdIdentifier",
                      "title" : "Secret ID Identifier",
                      "description" : "This identifier determines the secret ID for this
 entity provider when resolving secrets. For example when this value is set to \"demo\", the
 entity provider will use am.applications.federation.entity.providers.saml2.demo.signing and
 am.applications.federation.entity.providers.saml2.demo.encryption secret IDs to resolve the signing
 and encryption secrets. When left unspecified, AM will use the entity provider role (service
 provider, identity provider, etc.) specific default global secret IDs. When the secret ID identifier
 for a given role is modified, the corresponding mapping is removed if it isnâ##t referenced by other
 entities."
                    },
                    "signingAlgorithm" : {
                      "title" : "Signing Algorithm",
                      "type" : "array",
                      "attributePath" : {
                        "value" : "extensions",
                        "mapper" :
 "org.forgerock.openam.federation.rest.schema.mappers.SigningAlgorithmMapper"
                      },
                      "items" : {
                        "type" : "string",
                        "enum" : [ "http://www.w3.org/2000/09/xmldsig#rsa-sha1", "http://
www.w3.org/2001/04/xmldsig-more#ecdsa-sha256", "http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha384",
 "http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha512", "http://www.w3.org/2001/04/xmldsig-more#rsa-
sha256", "http://www.w3.org/2001/04/xmldsig-more#rsa-sha384", "http://www.w3.org/2001/04/xmldsig-
more#rsa-sha512", "http://www.w3.org/2009/xmldsig11#dsa-sha256" ],
                        "enumNames" : [ "http://www.w3.org/2000/09/xmldsig#rsa-sha1", "http://
www.w3.org/2001/04/xmldsig-more#ecdsa-sha256", "http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha384",
 "http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha512", "http://www.w3.org/2001/04/xmldsig-more#rsa-
sha256", "http://www.w3.org/2001/04/xmldsig-more#rsa-sha384", "http://www.w3.org/2001/04/xmldsig-
more#rsa-sha512", "http://www.w3.org/2009/xmldsig11#dsa-sha256" ]
                      }
                    },
                    "digestAlgorithm" : {
                      "title" : "Digest Algorithm",
                      "type" : "array",
                      "attributePath" : {
                        "value" : "extensions",
                        "mapper" :
 "org.forgerock.openam.federation.rest.schema.mappers.DigestAlgorithmMapper"
                      },
                      "items" : {
```

```
                        "type" : "string",
                        "enum" : [ "http://www.w3.org/2000/09/xmldsig#sha1", "http://
www.w3.org/2001/04/xmldsig-more#sha384", "http://www.w3.org/2001/04/xmlenc#sha256", "http://
www.w3.org/2001/04/xmlenc#sha512", "http://www.w3.org/2007/05/xmldsig-more#sha3-256", "http://
www.w3.org/2007/05/xmldsig-more#sha3-384", "http://www.w3.org/2007/05/xmldsig-more#sha3-512" ],
                        "enumNames" : [ "http://www.w3.org/2000/09/xmldsig#sha1", "http://
www.w3.org/2001/04/xmldsig-more#sha384", "http://www.w3.org/2001/04/xmlenc#sha256", "http://
www.w3.org/2001/04/xmlenc#sha512", "http://www.w3.org/2007/05/xmldsig-more#sha3-256", "http://
www.w3.org/2007/05/xmldsig-more#sha3-384", "http://www.w3.org/2007/05/xmldsig-more#sha3-512" ]
                      }
                    },
                    "encryptionAlgorithm" : {
                      "title" : "Encryption Algorithm",
                      "type" : "array",
                      "attributeKey" : {
                        "value" : "encryptionAlgorithms",
                        "mapper" :
 "org.forgerock.openam.federation.rest.schema.mappers.EncryptionAlgorithmMapper"
                      },
                      "items" : {
                        "type" : "string",
                        "enum" : [ "http://www.w3.org/2009/xmlenc11#aes128-gcm", "http://
www.w3.org/2009/xmlenc11#aes192-gcm", "http://www.w3.org/2009/xmlenc11#aes256-gcm", "http://
www.w3.org/2001/04/xmlenc#aes128-cbc", "http://www.w3.org/2001/04/xmlenc#aes192-cbc", "http://
www.w3.org/2001/04/xmlenc#aes256-cbc", "http://www.w3.org/2001/04/xmlenc#rsa-1_5", "http://
www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p", "http://www.w3.org/2009/xmlenc11#rsa-oaep" ],
                        "enumNames" : [ "http://www.w3.org/2009/xmlenc11#aes128-gcm", "http://
www.w3.org/2009/xmlenc11#aes192-gcm", "http://www.w3.org/2009/xmlenc11#aes256-gcm", "http://
www.w3.org/2001/04/xmlenc#aes128-cbc", "http://www.w3.org/2001/04/xmlenc#aes192-cbc", "http://
www.w3.org/2001/04/xmlenc#aes256-cbc", "http://www.w3.org/2001/04/xmlenc#rsa-1_5", "http://
www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p", "http://www.w3.org/2009/xmlenc11#rsa-oaep" ]
                      }
                    }
                  }
                }
              },
              "nameIdFormat" : {
                "traverseObject" : true,
                "title" : "NameID Format",
                "type" : "object",
                "properties" : {
                  "nameIdFormatList" : {
                    "description" : "List of NameID formats the requestor will use to contact. Order
 listed shows the order of preference",
                    "title" : "NameID Format List",
                    "attributePath" : {
                      "value" : "/nameIDFormat"
                    },
                    "type" : "array",
                    "items" : {
                      "type" : "string"
                    },
                    "default" : [ "urn:oasis:names:tc:SAML:2.0:nameid-format:persistent",
 "urn:oasis:names:tc:SAML:2.0:nameid-format:transient", "urn:oasis:names:tc:SAML:1.1:nameid-
format:emailAddress", "urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified",
 "urn:oasis:names:tc:SAML:1.1:nameid-format:WindowsDomainQualifiedName",
 "urn:oasis:names:tc:SAML:2.0:nameid-format:kerberos", "urn:oasis:names:tc:SAML:1.1:nameid-
format:X509SubjectName" ]
```

```
              },
              "disableNameIdPersistence" : {
                "attributeKey" : "spDoNotWriteFederationInfo",
                "title" : "Disable NameID persistence",
                "description" : "Instructs the SP to not persist the SAML NameID into the User
Data Store even if the NameID Format is urn:oasis:names:tc:SAML:2.0:nameid-format:persistent in the
received Assertion and the Account Mapper has identified the local user. When local authentication
is utilized for account linking purposes, enabling this feature will require end-users to locally
authenticate for each SAML-based login.",
                "type" : "boolean",
                "default" : false
              }
            }
          },
          "authenticationContext" : {
            "traverseObject" : true,
            "title" : "Authentication Context",
            "type" : "object",
            "properties" : {
              "authenticationContextMapper" : {
                "attributeKey" : "spAuthncontextMapper",
                "title" : "Mapper",
                "type" : "string",
                "default" : "com.sun.identity.saml2.plugins.DefaultSPAuthnContextMapper"
              },
              "authContextItems" : {
                "attributeKey" : {
                  "value" : "spAuthncontextClassrefMapping",
                  "mapper" :
"org.forgerock.openam.federation.rest.schema.mappers.SpAuthContextMapper"
                },
                "description" : "Defines mapping between IDP authentication context reference and
authentication level to be set on SP side session",
                "title" : "Authentication Context",
                "type" : "array",
                "items" : {
                  "type" : "object",
                  "properties" : {
                    "contextReference" : {
                      "propertyOrder" : 0,
                      "title" : "Context Reference",
                      "anyOf" : [ {
                        "title" : "Predefined Reference",
                        "type" : "string",
                        "enum" : [ "urn:oasis:names:tc:SAML:2.0:ac:classes:InternetProtocol",
"urn:oasis:names:tc:SAML:2.0:ac:classes:InternetProtocolPassword",
"urn:oasis:names:tc:SAML:2.0:ac:classes:Kerberos",
"urn:oasis:names:tc:SAML:2.0:ac:classes:MobileOneFactorUnregistered",
"urn:oasis:names:tc:SAML:2.0:ac:classes:MobileTwoFactorUnregistered",
"urn:oasis:names:tc:SAML:2.0:ac:classes:MobileOneFactorContract",
"urn:oasis:names:tc:SAML:2.0:ac:classes:MobileTwoFactorContract",
"urn:oasis:names:tc:SAML:2.0:ac:classes:Password",
"urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport",
"urn:oasis:names:tc:SAML:2.0:ac:classes:PreviousSession",
"urn:oasis:names:tc:SAML:2.0:ac:classes:X.509", "urn:oasis:names:tc:SAML:2.0:ac:classes:PGP",
"urn:oasis:names:tc:SAML:2.0:ac:classes:SPKI", "urn:oasis:names:tc:SAML:2.0:ac:classes:XMLDSig",
"urn:oasis:names:tc:SAML:2.0:ac:classes:Smartcard",
"urn:oasis:names:tc:SAML:2.0:ac:classes:SmartcardPKI",
"urn:oasis:names:tc:SAML:2.0:ac:classes:SoftwarePKI",
```

```
"urn:oasis:names:tc:SAML:2.0:ac:classes:Telephony",
"urn:oasis:names:tc:SAML:2.0:ac:classes:NomadTelephony",
"urn:oasis:names:tc:SAML:2.0:ac:classes:PersonalTelephony",
"urn:oasis:names:tc:SAML:2.0:ac:classes:AuthenticatedTelephony",
"urn:oasis:names:tc:SAML:2.0:ac:classes:SecureRemotePassword",
"urn:oasis:names:tc:SAML:2.0:ac:classes:TLSClient",
"urn:oasis:names:tc:SAML:2.0:ac:classes:TimeSyncToken", "unspecified" ],
                        "enumNames" : [ "InternetProtocol", "InternetProtocolPassword", "Kerberos",
"MobileOneFactorUnregistered", "MobileTwoFactorUnregistered", "MobileOneFactorContract",
"MobileTwoFactorContract", "Password", "PasswordProtectedTransport", "PreviousSession", "X.509",
"PGP", "SPKI", "XMLDSig", "Smartcard", "SmartcardPKI", "SoftwarePKI", "Telephony", "NomadTelephony",
"PersonalTelephony", "AuthenticatedTelephony", "SecureRemotePassword", "TLSClient", "TimeSyncToken",
"unspecified" ]
                      }, {
                        "title" : "Custom Reference",
                        "type" : "string"
                      } ]
                    },
                    "level" : {
                      "default" : 0,
                      "minimum" : 0,
                      "propertyOrder" : 1,
                      "title" : "Level",
                      "type" : "integer"
                    },
                    "defaultItem" : {
                      "propertyOrder" : 2,
                      "title" : "Default",
                      "type" : "boolean"
                    }
                  }
                },
                "default" : [ {
                  "contextReference" :
"urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport",
                  "level" : "0",
                  "defaultItem" : true
                } ]
              },
              "authenticationComparisonType" : {
                "attributeKey" : {
                  "value" : "spAuthncontextComparisonType",
                  "mapper" :
"org.forgerock.openam.federation.rest.schema.mappers.AuthComparisonTypeMapper"
                },
                "title" : "Comparison Type",
                "type" : "string",
                "enum" : [ "None", "Exact", "Minimum", "Maximum", "Better" ],
                "default" : "Exact"
              },
              "includeRequestedAuthenticationContext" : {
                "attributeKey" : "includeRequestedAuthnContext",
                "title" : "Include Request Authentication Context",
                "description" : "Enable to include the Requested Authentication Context in the
Authentication Request, enabled by default.",
                "type" : "boolean",
                "default" : true
              }
            }
```

```
            },
            "assertionTimeSkew" : {
              "attributeKey" : "assertionTimeSkew",
              "title" : "Assertion Time Skew",
              "description" : "Is in seconds. Skew time for NotBefore and NotOnOrAfter attributes in
assertion SubjectConfirmationData and Conditions",
              "type" : "integer",
              "default" : 300
            },
            "basicAuthentication" : {
              "traverseObject" : true,
              "description" : "Configure basic authentication setting for Soap based binding",
              "title" : "Basic Authentication",
              "type" : "object",
              "properties" : {
                "enabled" : {
                  "attributeKey" : "basicAuthOn",
                  "title" : "Enabled",
                  "type" : "boolean",
                  "default" : false
                },
                "userName" : {
                  "attributeKey" : "basicAuthUser",
                  "title" : "User Name",
                  "type" : "string"
                },
                "password" : {
                  "title" : "Password",
                  "attributeKey" : {
                    "value" : "basicAuthPassword",
                    "mapper" : "org.forgerock.openam.federation.rest.schema.mappers.PasswordMapper"
                  },
                  "type" : "string",
                  "format" : "password"
                }
              }
            }
          }
        },
        "assertionProcessing" : {
          "propertyOrder" : 1,
          "traverseObject" : true,
          "title" : "Assertion Processing",
          "type" : "object",
          "properties" : {
            "attributeMapper" : {
              "traverseObject" : true,
              "title" : "Attribute Mapper",
              "type" : "object",
              "properties" : {
                "attributeMapper" : {
                  "attributeKey" : "spAttributeMapper",
                  "title" : "Attribute Mapper",
                  "type" : "string",
                  "default" : "com.sun.identity.saml2.plugins.DefaultSPAttributeMapper"
                },
                "attributeMap" : {
                  "attributeKey" : {
                    "value" : "attributeMap",
```

```
                  "mapper" : "org.forgerock.openam.federation.rest.schema.mappers.KeyValueMapper"
                },
                "description" : "This mapping is the configuration used by the Attribute Mapper.
Mapping should be defined as SAML ATTRIBUTE NAME=PROFILE ATTRIBUTE NAME in assertion. Example:
EmailAddress=mail, Address=postaladdress.",
                "title" : "Attribute Map",
                "type" : "array",
                "items" : {
                  "type" : "object",
                  "properties" : {
                    "key" : {
                      "propertyOrder" : 0,
                      "title" : "Key",
                      "type" : "string"
                    },
                    "value" : {
                      "propertyOrder" : 1,
                      "title" : "Value",
                      "type" : "string"
                    }
                  }
                },
                "default" : [ {
                  "key" : "*",
                  "value" : "*"
                } ]
              }
            },
            "required" : [ "attributeMapper" ]
          },
          "autoFederation" : {
            "description" : "Enable Auto Federation if not already federated",
            "traverseObject" : true,
            "title" : "Auto Federation",
            "type" : "object",
            "properties" : {
              "autoFedEnabled" : {
                "attributeKey" : "autofedEnabled",
                "title" : "Enabled",
                "description" : "Enable Auto Federation if not already federated",
                "type" : "boolean",
                "default" : false
              },
              "autoFedAttribute" : {
                "attributeKey" : "autofedAttribute",
                "title" : "Attribute",
                "description" : "This SAML attribute identifies the user to auto federate with. If
this attribute is not present in the assertion then the value of the NameID is used instead. If there
is a mapping defined for this attribute, it will be used along with the value when searching for the
local user. If the local user can not be found and Dynamic or Ignored Profile is enabled, the value
will be used as the local user's UID instead.",
                "type" : "string"
              }
            }
          },
          "accountMapping" : {
            "traverseObject" : true,
            "title" : "Account Mapper",
            "type" : "object",
```

```
            "properties" : {
              "spAccountMapper" : {
                "attributeKey" : "spAccountMapper",
                "title" : "Account Mapper",
                "description" : "Helps to find the user on local side based on incoming assertion",
                "type" : "string",
                "default" : "com.sun.identity.saml2.plugins.DefaultSPAccountMapper"
              },
              "useNameIDAsSPUserID" : {
                "attributeKey" : "useNameIDAsSPUserID",
                "title" : "Use Name ID as User ID",
                "description" : "Use value of Name ID from the incoming Assertion to find the local
user as the final resort, if other means do not apply",
                "type" : "boolean",
                "default" : false
              },
              "transientUser" : {
                "attributeKey" : "transientUser",
                "description" : "Can be null. If specified this will be the mapped SP user incase of
transient federation",
                "title" : "Transient User",
                "type" : "string"
              }
            }
          },
          "responseArtifactMessageEncoding" : {
            "traverseObject" : true,
            "title" : "Artifact Message Encoding",
            "type" : "object",
            "properties" : {
              "encoding" : {
                "attributeKey" : {
                  "value" : "responseArtifactMessageEncoding",
                  "mapper" :
"org.forgerock.openam.federation.rest.schema.mappers.MessageEncodingMapper"
                },
                "title" : "Artifact Message Encoding",
                "type" : "string",
                "enum" : [ "URI", "FORM" ],
                "default" : "URI"
              }
            }
          },
          "url" : {
            "traverseObject" : true,
            "title" : "URL",
            "type" : "object",
            "properties" : {
              "localAuthUrl" : {
                "attributeKey" : "localAuthURL",
                "title" : "Local Authentication Url",
                "description" : "For local authentication",
                "type" : "string"
              },
              "intermediateUrl" : {
                "attributeKey" : "intermediateUrl",
                "title" : "Intermediate Url",
                "description" : "This is the intermediate point that SP will redirect to before the
final relay state",
```

```
                "type" : "string"
              },
              "appLogoutUrl" : {
                "attributeKey" : "appLogoutUrl",
                "title" : "External Application Logout URL",
                "description" : "This is the logout URL for an external application. Once the server
receives logout request from the remote partner, a request will be sent to the logout URL using back
channel HTTP POST with all cookies. Optionally, a user session property could be sent as HTTP header
and POST parameter if a query parameter \"appsessionproperty\" (set to the session property name) is
included in the URL. e.g. \"http://www.app.domain.com/uri/logout?appsessionproperty=mail\"",
                "type" : "string"
              }
            }
          },
          "defaultRelayState" : {
            "attributeKey" : "defaultRelayState",
            "title" : "Default Relay State Url",
            "description" : "This is the default relay state URL that the SP will redirect to, in
case there is no relay state specified in the response",
            "type" : "string"
          },
          "adapter" : {
            "traverseObject" : true,
            "title" : "Adapter",
            "type" : "object",
            "properties" : {
              "spAdapter" : {
                "attributeKey" : "spAdapter",
                "title" : "Adapter",
                "description" : "Implementation class for the SAML2ServiceProviderAdapter which is
used to add application specific processing logic during federation process",
                "type" : "string"
              },
              "spAdapterEnv" : {
                "attributeKey" : {
                  "value" : "spAdapterEnv",
                  "mapper" : "org.forgerock.openam.federation.rest.schema.mappers.KeyValueMapper"
                },
                "title" : "Adapter Environment",
                "type" : "array",
                "items" : {
                  "type" : "object",
                  "properties" : {
                    "key" : {
                      "propertyOrder" : 0,
                      "title" : "Key",
                      "type" : "string"
                    },
                    "value" : {
                      "propertyOrder" : 1,
                      "title" : "Value",
                      "type" : "string"
                    }
                  }
                }
              }
            }
          }
        }
```

```
      },
      "services" : {
        "propertyOrder" : 2,
        "traverseObject" : true,
        "type" : "object",
        "title" : "Services",
        "properties" : {
          "metaAlias" : {
            "attributeKey" : "metaAlias",
            "default" : "{spMetaAlias}",
            "title" : "MetaAlias",
            "description" : "The MetaAlias attribute is specific to providers using OpenAM
therefore, a null value for a remote provider configuration is possible.",
            "type" : "string",
            "readOnly" : true
          },
          "serviceAttributes" : {
            "traverseObject" : true,
            "title" : "SP Service Attributes",
            "type" : "object",
            "properties" : {
              "singleLogoutService" : {
                "title" : "Single Logout Service",
                "type" : "array",
                "attributePath" : {
                  "value" : "singleLogoutService",
                  "mapper" : "org.forgerock.openam.federation.rest.schema.mappers.EndpointMapper"
                },
                "items" : {
                  "type" : "object",
                  "properties" : {
                    "binding" : {
                      "title" : "Binding",
                      "anyOf" : [ {
                        "title" : "Predefined Binding",
                        "type" : "string",
                        "enum" : [ "urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect",
"urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST", "urn:oasis:names:tc:SAML:2.0:bindings:SOAP",
"urn:oasis:names:tc:SAML:2.0:bindings:PAOS" ],
                        "enumNames" : [ "HTTP-REDIRECT", "HTTP-POST", "SOAP", "PAOS" ]
                      }, {
                        "title" : "Custom Binding",
                        "type" : "string"
                      } ]
                    },
                    "location" : {
                      "title" : "Location",
                      "type" : "string"
                    },
                    "responseLocation" : {
                      "title" : "Response Location",
                      "type" : "string"
                    }
                  },
                  "required" : [ "location" ]
                },
                "default" : [ {
                  "binding" : "urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect",
                  "location" : "{baseUrl}/SPSloRedirect/metaAlias{spMetaAlias}",
```

```
                    "responseLocation" : "{baseUrl}/SPSloRedirect/metaAlias{spMetaAlias}"
                  }, {
                    "binding" : "urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST",
                    "location" : "{baseUrl}/SPSloPOST/metaAlias{spMetaAlias}",
                    "responseLocation" : "{baseUrl}/SPSloPOST/metaAlias{spMetaAlias}"
                  }, {
                    "binding" : "urn:oasis:names:tc:SAML:2.0:bindings:SOAP",
                    "location" : "{baseUrl}/SPSloSoap/metaAlias{spMetaAlias}"
                  } ]
                },
                "nameIdService" : {
                  "title" : "Manage NameID Service",
                  "type" : "array",
                  "attributePath" : {
                    "value" : "manageNameIDService",
                    "mapper" : "org.forgerock.openam.federation.rest.schema.mappers.EndpointMapper"
                  },
                  "items" : {
                    "type" : "object",
                    "properties" : {
                      "binding" : {
                        "title" : "Binding",
                        "anyOf" : [ {
                          "title" : "Predefined Binding",
                          "type" : "string",
                          "enum" : [ "urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect",
"urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST", "urn:oasis:names:tc:SAML:2.0:bindings:SOAP",
"urn:oasis:names:tc:SAML:2.0:bindings:PAOS" ],
                          "enumNames" : [ "HTTP-REDIRECT", "HTTP-POST", "SOAP", "PAOS" ]
                        }, {
                          "title" : "Custom Binding",
                          "type" : "string"
                        } ]
                      },
                      "location" : {
                        "title" : "Location",
                        "type" : "string"
                      },
                      "responseLocation" : {
                        "title" : "Response Location",
                        "type" : "string"
                      }
                    },
                    "required" : [ "location" ]
                  },
                  "default" : [ {
                    "binding" : "urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect",
                    "location" : "{baseUrl}/SPMniRedirect/metaAlias{spMetaAlias}",
                    "responseLocation" : "{baseUrl}/SPMniRedirect/metaAlias{spMetaAlias}"
                  }, {
                    "binding" : "urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST",
                    "location" : "{baseUrl}/SPMniPOST/metaAlias{spMetaAlias}",
                    "responseLocation" : "{baseUrl}/SPMniPOST/metaAlias{spMetaAlias}"
                  }, {
                    "binding" : "urn:oasis:names:tc:SAML:2.0:bindings:SOAP",
                    "location" : "{baseUrl}/SPMniSoap/metaAlias{spMetaAlias}",
                    "responseLocation" : "{baseUrl}/SPMniSoap/metaAlias{spMetaAlias}"
                  } ]
                },
```

```
                "assertionConsumerService" : {
                  "attributePath" : {
                    "value" : "assertionConsumerService",
                    "mapper" :
"org.forgerock.openam.federation.rest.schema.mappers.ExtendedIndexedEndpointMapper"
                  },
                  "title" : "Assertion Consumer Service",
                  "description" : "Location denotes the URL to accept the respective request type.
Index denotes the index of the URL in the standard metadata",
                  "type" : "array",
                  "items" : {
                    "type" : "object",
                    "properties" : {
                      "isDefault" : {
                        "type" : "boolean"
                      },
                      "binding" : {
                        "title" : "Binding",
                        "anyOf" : [ {
                          "title" : "Predefined Binding",
                          "type" : "string",
                          "enum" : [ "urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Artifact",
"urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST", "urn:oasis:names:tc:SAML:2.0:bindings:PAOS" ],
                          "enumNames" : [ "HTTP-Artifact", "HTTP-POST", "PAOS" ]
                        }, {
                          "title" : "Custom Binding",
                          "type" : "string"
                        } ]
                      },
                      "location" : {
                        "title" : "Location",
                        "type" : "string"
                      },
                      "index" : {
                        "type" : "integer"
                      }
                    }
                  },
                  "default" : [ {
                    "isDefault" : true,
                    "binding" : "urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Artifact",
                    "location" : "{baseUrl}/Consumer/metaAlias{spMetaAlias}",
                    "index" : "0"
                  }, {
                    "isDefault" : false,
                    "binding" : "urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST",
                    "location" : "{baseUrl}/Consumer/metaAlias{spMetaAlias}",
                    "index" : "1"
                  }, {
                    "isDefault" : false,
                    "binding" : "urn:oasis:names:tc:SAML:2.0:bindings:PAOS",
                    "location" : "{baseUrl}/Consumer/ECP/metaAlias{spMetaAlias}",
                    "index" : "2"
                  } ]
                }
              }
            }
          }
        },
```

```
       "advanced" : {
         "propertyOrder" : 3,
         "traverseObject" : true,
         "type" : "object",
         "title" : "Advanced",
         "properties" : {
           "saeConfiguration" : {
             "traverseObject" : true,
             "title" : "SAE Configuration",
             "type" : "object",
             "properties" : {
               "spUrl" : {
                 "attributeKey" : "saeSPUrl",
                 "title" : "SP URL",
                 "description" : "URL endpoint on Service Provider that can handle SAE requests.
If this URL is empty (not configured), SAE single sign-on will not be enabled. Normal samlv2 single
sign-on response will be sent to SP",
                 "type" : "string",
                 "default" : "{baseUrl}/spsaehandler/metaAlias{spMetaAlias}"
               },
               "spLogoutUrl" : {
                 "attributeKey" : "saeSPLogoutUrl",
                 "title" : "SP Logout URL",
                 "description" : "URL endpoint on the Service Provider that can handle SAE global
logout requests",
                 "type" : "string"
               },
               "applicationSecurityConfiguration" : {
                 "attributeKey" : {
                   "value" : "saeAppSecretList",
                   "mapper" :
"org.forgerock.openam.federation.rest.schema.mappers.ApplicationSecurityConfigItemMapper"
                 },
                 "title" : "Application Security Configuration",
                 "type" : "array",
                 "items" : {
                   "type" : "object",
                   "properties" : {
                     "url" : {
                       "title" : "URL",
                       "propertyOrder" : 0,
                       "type" : "string"
                     },
                     "type" : {
                       "title" : "Type",
                       "propertyOrder" : 1,
                       "type" : "string"
                     },
                     "pubKeyAlias" : {
                       "title" : "Public Key Alias",
                       "propertyOrder" : 2,
                       "type" : "string"
                     },
                     "encryptionAlgorithm" : {
                       "title" : "Encryption Algorithm",
                       "propertyOrder" : 3,
                       "type" : "string"
                     },
                     "encryptionKeyStrength" : {
```

```
                      "title" : "Encryption Key Strength",
                      "propertyOrder" : 4,
                      "type" : "string"
                    },
                    "secret" : {
                      "title" : "Secret",
                      "propertyOrder" : 5,
                      "type" : "string"
                    }
                  },
                  "required" : [ "url", "secret" ]
                }
              }
            }
          },
          "ecpConfiguration" : {
            "traverseObject" : true,
            "title" : "ECP Configuration",
            "type" : "object",
            "properties" : {
              "ecpRequestIdpListFinderImpl" : {
                "attributeKey" : "ECPRequestIDPListFinderImpl",
                "title" : "Request IDP List Finder Implementation",
                "description" : "Implementation class of the IDP list finder SPI. This returns a
list of preferred IDPs trusted by the ECP",
                "type" : "string",
                "default" : "com.sun.identity.saml2.plugins.ECPIDPFinder"
              },
              "ecpRequestIdpListGetComplete" : {
                "attributeKey" : "ECPRequestIDPListGetComplete",
                "title" : "Request IDP List Get Complete",
                "description" : "Specify an URI reference that can be used to retrieve the complete
IDP list if the IDPList element is not complete",
                "type" : "string"
              },
              "ecpRequestIdpList" : {
                "attributeKey" : "ECPRequestIDPList",
                "title" : "Request IDP List",
                "description" : "Defines a list of IDPs for the ECP to contact. This is used by the
default implementation of the IDP Finder",
                "type" : "array",
                "items" : {
                  "type" : "string"
                }
              }
            }
          },
          "idpProxy" : {
            "traverseObject" : true,
            "title" : "IDP Proxy",
            "type" : "object",
            "properties" : {
              "enableIdpProxy" : {
                "attributeKey" : "enableIDPProxy",
                "title" : "IDP Proxy enabled",
                "description" : "Enable IDP Proxy if not enabled",
                "type" : "boolean",
                "default" : false
              },
```

```
                "useIntroductionForIdpProxy" : {
                  "attributeKey" : "useIntroductionForIDPProxy",
                  "title" : "Introduction enabled",
                  "type" : "boolean",
                  "default" : false
                },
                "idpProxyCount" : {
                  "attributeKey" : "idpProxyCount",
                  "title" : "Proxy Count",
                  "description" : "Number of IDP proxies that the SP can have",
                  "type" : "integer",
                  "default" : 0
                },
                "idpProxyList" : {
                  "attributeKey" : "idpProxyList",
                  "description" : "A list of preferred IDPs that the SP would proxy to",
                  "title" : "IDP Proxy List",
                  "type" : "array",
                  "items" : {
                    "type" : "string"
                  }
                }
              }
            },
            "spSessionSyncEnabled" : {
              "attributeKey" : "spSessionSyncEnabled",
              "title" : "Session Synchronization",
              "description" : "If this is enabled, when a session times out, the Service Provider
 notifies all Identity Providers to log out. A session may time out, for example, when max-idle time
 or max-session time is reached.",
              "type" : "boolean",
              "default" : false
            },
            "relayStateUrlList" : {
              "traverseObject" : true,
              "title" : "Relay State URL List",
              "type" : "object",
              "properties" : {
                "relayStateUrlList" : {
                  "attributeKey" : "relayStateUrlList",
                  "title" : "Relay State URL List",
                  "type" : "array",
                  "items" : {
                    "type" : "string"
                  }
                }
              }
            }
          }
        }
      }
    }
  },
  "required" : [ "entityId" ],
  "$id" : "https://www.forgerock.com/hostedSaml2EntityProvider.schema.json"
}
```

delete

Removes the SAML2 entity provider from the configuration including all of its associated roles.

Usage:

```
am> delete HostedSaml2EntityProvider --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

read

Returns the roles of the SAML2 entity provider.

Usage:

```
am> read HostedSaml2EntityProvider --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Updates details of the SAML2 entity provider role.

Usage:

```
am> update HostedSaml2EntityProvider --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "$schema" : "http://json-schema.org/draft-07/schema#",
  "ignoredProperties" : [ "_id", "_rev" ],
  "description" : "This schema describes a hosted SAML2 entity provider.",
  "title" : "SAML2 Hosted Entity Provider",
  "type" : "object",
  "properties" : {
    "entityId" : {
      "type" : "string"
```

```
    },
    "identityProvider" : {
      "title" : "Identity Provider",
      "description" : "This schema describes a SAML2 identity provider.",
      "type" : "object",
      "traverseObject" : true,
      "properties" : {
        "assertionContent" : {
          "propertyOrder" : 0,
          "title" : "Assertion Content",
          "type" : "object",
          "traverseObject" : true,
          "properties" : {
            "signingAndEncryption" : {
              "traverseObject" : true,
              "title" : "Signing And Encryption",
              "type" : "object",
              "properties" : {
                "requestResponseSigning" : {
                  "traverseObject" : true,
                  "title" : "Request/Response Signing",
                  "description" : "Select the checkbox for each request/response that should be
signed",
                  "type" : "object",
                  "properties" : {
                    "authenticationRequest" : {
                      "attributePath" : {
                        "value" : "/wantAuthnRequestsSigned"
                      },
                      "title" : "Authentication Request",
                      "type" : "boolean",
                      "default" : false
                    },
                    "artifactResolve" : {
                      "attributeKey" : "wantArtifactResolveSigned",
                      "title" : "Artifact Resolve",
                      "type" : "boolean",
                      "default" : false
                    },
                    "logoutRequest" : {
                      "attributeKey" : "wantLogoutRequestSigned",
                      "title" : "Logout Request",
                      "type" : "boolean",
                      "default" : false
                    },
                    "logoutResponse" : {
                      "attributeKey" : "wantLogoutResponseSigned",
                      "title" : "Logout Response",
                      "type" : "boolean",
                      "default" : false
                    },
                    "manageNameIdRequest" : {
                      "attributeKey" : "wantMNIRequestSigned",
                      "title" : "Manage NameID Request",
                      "type" : "boolean",
                      "default" : false
                    },
                    "manageNameIdResponse" : {
                      "attributeKey" : "wantMNIResponseSigned",
```

```
                    "title" : "Manage NameID Response",
                    "type" : "boolean",
                    "default" : false
                  }
                },
                "required" : [ "authenticationRequest", "artifactResolve", "logoutRequest",
 "logoutResponse", "manageNameIdRequest", "manageNameIdResponse" ]
              },
              "encryption" : {
                "traverseObject" : true,
                "title" : "Encryption",
                "type" : "object",
                "properties" : {
                  "nameIdEncryption" : {
                    "attributeKey" : "wantNameIDEncrypted",
                    "title" : "NameID Encryption",
                    "type" : "boolean",
                    "default" : false
                  }
                },
                "required" : [ "nameIdEncryption" ]
              },
              "secretIdAndAlgorithms" : {
                "traverseObject" : true,
                "title" : "Secret ID And Algorithms",
                "type" : "object",
                "properties" : {
                  "secretIdIdentifier" : {
                    "type" : "string",
                    "attributeKey" : "secretIdIdentifier",
                    "title" : "Secret ID Identifier",
                    "description" : "This identifier determines the secret ID for this
 entity provider when resolving secrets. For example when this value is set to \"demo\", the
 entity provider will use am.applications.federation.entity.providers.saml2.demo.signing and
 am.applications.federation.entity.providers.saml2.demo.encryption secret IDs to resolve the signing
 and encryption secrets. When left unspecified, AM will use the entity provider role (service
 provider, identity provider, etc.) specific default global secret IDs. When the secret ID identifier
 for a given role is modified, the corresponding mapping is removed if it isnâ##t referenced by other
 entities."
                  },
                  "signingAlgorithm" : {
                    "title" : "Signing Algorithm",
                    "type" : "array",
                    "attributePath" : {
                      "value" : "extensions",
                      "mapper" :
 "org.forgerock.openam.federation.rest.schema.mappers.SigningAlgorithmMapper"
                    },
                    "items" : {
                      "type" : "string",
                      "enum" : [ "http://www.w3.org/2000/09/xmldsig#rsa-sha1", "http://
www.w3.org/2001/04/xmldsig-more#ecdsa-sha256", "http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha384",
 "http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha512", "http://www.w3.org/2001/04/xmldsig-more#rsa-
sha256", "http://www.w3.org/2001/04/xmldsig-more#rsa-sha384", "http://www.w3.org/2001/04/xmldsig-
more#rsa-sha512", "http://www.w3.org/2009/xmldsig11#dsa-sha256" ],
                      "enumNames" : [ "http://www.w3.org/2000/09/xmldsig#rsa-sha1", "http://
www.w3.org/2001/04/xmldsig-more#ecdsa-sha256", "http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha384",
 "http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha512", "http://www.w3.org/2001/04/xmldsig-more#rsa-
```

```
sha256", "http://www.w3.org/2001/04/xmldsig-more#rsa-sha384", "http://www.w3.org/2001/04/xmldsig-
more#rsa-sha512", "http://www.w3.org/2009/xmldsig11#dsa-sha256" ]
                      }
                    },
                    "digestAlgorithm" : {
                      "title" : "Digest Algorithm",
                      "type" : "array",
                      "attributePath" : {
                        "value" : "extensions",
                        "mapper" :
 "org.forgerock.openam.federation.rest.schema.mappers.DigestAlgorithmMapper"
                      },
                      "items" : {
                        "type" : "string",
                        "enum" : [ "http://www.w3.org/2000/09/xmldsig#sha1", "http://
www.w3.org/2001/04/xmldsig-more#sha384", "http://www.w3.org/2001/04/xmlenc#sha256", "http://
www.w3.org/2001/04/xmlenc#sha512", "http://www.w3.org/2007/05/xmldsig-more#sha3-256", "http://
www.w3.org/2007/05/xmldsig-more#sha3-384", "http://www.w3.org/2007/05/xmldsig-more#sha3-512" ],
                        "enumNames" : [ "http://www.w3.org/2000/09/xmldsig#sha1", "http://
www.w3.org/2001/04/xmldsig-more#sha384", "http://www.w3.org/2001/04/xmlenc#sha256", "http://
www.w3.org/2001/04/xmlenc#sha512", "http://www.w3.org/2007/05/xmldsig-more#sha3-256", "http://
www.w3.org/2007/05/xmldsig-more#sha3-384", "http://www.w3.org/2007/05/xmldsig-more#sha3-512" ]
                      }
                    },
                    "encryptionAlgorithm" : {
                      "title" : "Encryption Algorithm",
                      "type" : "array",
                      "attributeKey" : {
                        "value" : "encryptionAlgorithms",
                        "mapper" :
 "org.forgerock.openam.federation.rest.schema.mappers.EncryptionAlgorithmMapper"
                      },
                      "items" : {
                        "type" : "string",
                        "enum" : [ "http://www.w3.org/2009/xmlenc11#aes128-gcm", "http://
www.w3.org/2009/xmlenc11#aes192-gcm", "http://www.w3.org/2009/xmlenc11#aes256-gcm", "http://
www.w3.org/2001/04/xmlenc#aes128-cbc", "http://www.w3.org/2001/04/xmlenc#aes192-cbc", "http://
www.w3.org/2001/04/xmlenc#aes256-cbc", "http://www.w3.org/2001/04/xmlenc#rsa-1_5", "http://
www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p", "http://www.w3.org/2009/xmlenc11#rsa-oaep" ],
                        "enumNames" : [ "http://www.w3.org/2009/xmlenc11#aes128-gcm", "http://
www.w3.org/2009/xmlenc11#aes192-gcm", "http://www.w3.org/2009/xmlenc11#aes256-gcm", "http://
www.w3.org/2001/04/xmlenc#aes128-cbc", "http://www.w3.org/2001/04/xmlenc#aes192-cbc", "http://
www.w3.org/2001/04/xmlenc#aes256-cbc", "http://www.w3.org/2001/04/xmlenc#rsa-1_5", "http://
www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p", "http://www.w3.org/2009/xmlenc11#rsa-oaep" ]
                      }
                    }
                  }
                }
              }
            },
            "nameIdFormat" : {
              "traverseObject" : true,
              "title" : "NameID Format",
              "type" : "object",
              "properties" : {
                "nameIdFormatList" : {
                  "description" : "List of NameID formats the requestor will use to contact. Order
 listed shows the order of preference",
                  "title" : "NameID Format List",
```

```
                  "attributePath" : {
                    "value" : "/nameIDFormat"
                  },
                  "type" : "array",
                  "items" : {
                    "type" : "string"
                  },
                  "default" : [ "urn:oasis:names:tc:SAML:2.0:nameid-format:persistent",
 "urn:oasis:names:tc:SAML:2.0:nameid-format:transient", "urn:oasis:names:tc:SAML:1.1:nameid-
format:emailAddress", "urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified",
 "urn:oasis:names:tc:SAML:1.1:nameid-format:WindowsDomainQualifiedName",
 "urn:oasis:names:tc:SAML:2.0:nameid-format:kerberos", "urn:oasis:names:tc:SAML:1.1:nameid-
format:X509SubjectName" ]
                },
                "nameIdValueMap" : {
                  "attributeKey" : {
                    "value" : "nameIDFormatMap",
                    "mapper" : "org.forgerock.openam.federation.rest.schema.mappers.NameIdValueMapper"
                  },
                  "description" : "Defines mapping between the NameID format and user's profile
 attribute. Example <code>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress=mail</code> or
 <code>urn:oasis:names:tc:SAML:2.0:nameid-format:persistent=objectGUID;binary</code>. If the defined
 NameID format is used in protocol, the profile attribute value will be used as NameID value for
 the format in the Subject, the <code>;binary</code> flag can be used to indicate that the profile
 attribute is binary and should be Base64 encoded when used as the NameID value.",
                  "title" : "NameID Value Map",
                  "type" : "array",
                  "items" : {
                    "type" : "object",
                    "properties" : {
                      "key" : {
                        "title" : "Key",
                        "propertyOrder" : 0,
                        "type" : "string"
                      },
                      "value" : {
                        "title" : "Value",
                        "propertyOrder" : 1,
                        "type" : "string"
                      },
                      "binary" : {
                        "title" : "Binary",
                        "propertyOrder" : 2,
                        "type" : "boolean"
                      }
                    }
                  },
                  "default" : [ {
                    "key" : "urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress",
                    "value" : "mail",
                    "binary" : false
                  } ]
                }
              }
            },
            "authenticationContext" : {
              "title" : "Authentication Context",
              "type" : "object",
              "traverseObject" : true,
```

```
            "properties" : {
              "authenticationContextMapper" : {
                "attributeKey" : "idpAuthncontextMapper",
                "title" : "Mapper",
                "type" : "string",
                "default" : "com.sun.identity.saml2.plugins.DefaultIDPAuthnContextMapper"
              },
              "authContextItems" : {
                "title" : "Authentication Context",
                "description" : "Defines mapping between SP requested Authentication Context
Reference and IDP authentication scheme and authentication level.",
                "type" : "array",
                "attributeKey" : {
                  "value" : "idpAuthncontextClassrefMapping",
                  "mapper" :
"org.forgerock.openam.federation.rest.schema.mappers.IdpAuthContextMapper"
                },
                "items" : {
                  "type" : "object",
                  "properties" : {
                    "contextReference" : {
                      "propertyOrder" : 0,
                      "title" : "Context Reference",
                      "anyOf" : [ {
                        "title" : "Predefined Reference",
                        "type" : "string",
                        "enum" : [ "urn:oasis:names:tc:SAML:2.0:ac:classes:InternetProtocol",
"urn:oasis:names:tc:SAML:2.0:ac:classes:InternetProtocolPassword",
"urn:oasis:names:tc:SAML:2.0:ac:classes:Kerberos",
"urn:oasis:names:tc:SAML:2.0:ac:classes:MobileOneFactorUnregistered",
"urn:oasis:names:tc:SAML:2.0:ac:classes:MobileTwoFactorUnregistered",
"urn:oasis:names:tc:SAML:2.0:ac:classes:MobileOneFactorContract",
"urn:oasis:names:tc:SAML:2.0:ac:classes:MobileTwoFactorContract",
"urn:oasis:names:tc:SAML:2.0:ac:classes:Password",
"urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport",
"urn:oasis:names:tc:SAML:2.0:ac:classes:PreviousSession",
"urn:oasis:names:tc:SAML:2.0:ac:classes:X.509", "urn:oasis:names:tc:SAML:2.0:ac:classes:PGP",
"urn:oasis:names:tc:SAML:2.0:ac:classes:SPKI", "urn:oasis:names:tc:SAML:2.0:ac:classes:XMLDSig",
"urn:oasis:names:tc:SAML:2.0:ac:classes:Smartcard",
"urn:oasis:names:tc:SAML:2.0:ac:classes:SmartcardPKI",
"urn:oasis:names:tc:SAML:2.0:ac:classes:SoftwarePKI",
"urn:oasis:names:tc:SAML:2.0:ac:classes:Telephony",
"urn:oasis:names:tc:SAML:2.0:ac:classes:NomadTelephony",
"urn:oasis:names:tc:SAML:2.0:ac:classes:PersonalTelephony",
"urn:oasis:names:tc:SAML:2.0:ac:classes:AuthenticatedTelephony",
"urn:oasis:names:tc:SAML:2.0:ac:classes:SecureRemotePassword",
"urn:oasis:names:tc:SAML:2.0:ac:classes:TLSClient",
"urn:oasis:names:tc:SAML:2.0:ac:classes:TimeSyncToken", "unspecified" ],
                        "enumNames" : [ "InternetProtocol", "InternetProtocolPassword", "Kerberos",
"MobileOneFactorUnregistered", "MobileTwoFactorUnregistered", "MobileOneFactorContract",
"MobileTwoFactorContract", "Password", "PasswordProtectedTransport", "PreviousSession", "X.509",
"PGP", "SPKI", "XMLDSig", "Smartcard", "SmartcardPKI", "SoftwarePKI", "Telephony", "NomadTelephony",
"PersonalTelephony", "AuthenticatedTelephony", "SecureRemotePassword", "TLSClient", "TimeSyncToken",
"unspecified" ]
                      }, {
                        "title" : "Custom Reference",
                        "type" : "string"
                      } ]
                    },
```

```
                    "key" : {
                      "propertyOrder" : 1,
                      "type" : "string",
                      "title" : "Key",
                      "enum" : [ "service", "module", "user", "role", "authlevel" ],
                      "enumNames" : [ "Service", "Module", "User", "Role", "Authentication Level" ]
                    },
                    "value" : {
                      "propertyOrder" : 2,
                      "title" : "Value",
                      "type" : "string"
                    },
                    "level" : {
                      "propertyOrder" : 3,
                      "title" : "Level",
                      "type" : "integer",
                      "minimum" : 0
                    }
                  }
                },
                "default" : [ {
                  "contextReference" :
"urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport",
                  "level" : "0"
                } ]
              }
            }
          },
          "assertionTime" : {
            "traverseObject" : true,
            "title" : "Assertion Time",
            "type" : "object",
            "properties" : {
              "notBeforeTimeSkew" : {
                "attributeKey" : "assertionNotBeforeTimeSkew",
                "title" : "Not-Before Time Skew",
                "type" : "integer",
                "minimum" : 0,
                "default" : 600,
                "description" : "Is in seconds. This is the skew time for NotBefore attributes in
assertion"
              },
              "effectiveTime" : {
                "attributeKey" : "assertionEffectiveTime",
                "title" : "Effective Time",
                "type" : "integer",
                "minimum" : 0,
                "description" : "Is in seconds. Validity time of assertion for NotAfter attributes",
                "default" : 600
              }
            }
          },
          "basicAuthentication" : {
            "traverseObject" : true,
            "description" : "Configure basic authentication setting for Soap based binding",
            "title" : "Basic Authentication",
            "type" : "object",
            "properties" : {
              "enabled" : {
```

```
                  "attributeKey" : "basicAuthOn",
                  "title" : "Enabled",
                  "type" : "boolean",
                  "default" : false
                },
                "userName" : {
                  "attributeKey" : "basicAuthUser",
                  "title" : "User Name",
                  "type" : "string"
                },
                "password" : {
                  "title" : "Password",
                  "attributeKey" : {
                    "value" : "basicAuthPassword",
                    "mapper" : "org.forgerock.openam.federation.rest.schema.mappers.PasswordMapper"
                  },
                  "type" : "string",
                  "format" : "password"
                }
              }
            },
            "assertionCache" : {
              "traverseObject" : true,
              "type" : "object",
              "title" : "Assertion Cache",
              "properties" : {
                "enabled" : {
                  "attributeKey" : "assertionCacheEnabled",
                  "description" : "Enable assertion cache",
                  "title" : "Enabled",
                  "type" : "boolean",
                  "default" : false
                }
              }
            }
          }
        },
        "assertionProcessing" : {
          "propertyOrder" : 1,
          "title" : "Assertion Processing",
          "type" : "object",
          "traverseObject" : true,
          "properties" : {
            "attributeMapper" : {
              "title" : "Attribute Mapper",
              "type" : "object",
              "traverseObject" : true,
              "properties" : {
                "attributeMapper" : {
                  "attributeKey" : "idpAttributeMapper",
                  "title" : "Attribute Mapper",
                  "type" : "string",
                  "default" : "com.sun.identity.saml2.plugins.DefaultIDPAttributeMapper"
                },
                "attributeMap" : {
                  "title" : "Attribute Map",
                  "description" : "This mapping is the configuration used by the Attribute Mapper.
The mapping should be defined as [NameFormatURI|]SAML ATTRIBUTE NAME=PROFILE ATTRIBUTE NAME in
assertion. Example: EmailAddress=mail, Address=postaladdress, urn:oasis:names:tc:SAML:2.0:attrname-
```

```
format:uri|urn:mace:dir:attribute-def:cn=cn The mapper also allows for static values to be defined.
 To define a static value, enclose the profile attribute name in double quotes. Example: partnerID=
\"staticPartnerIDValue\", urn:oasis:names:tc:SAML:2.0:attrname-format:uri|nameID=\"staticNameIDValue
\". To flag an attribute as being a binary value and have its value Base64 encoded, add ;binary to the
 end of the profile attribute name. Example: photo=photo;binary, urn:oasis:names:tc:SAML:2.0:attrname-
format:uri|photo=photo;binary",
                  "type" : "array",
                  "attributeKey" : {
                    "value" : "attributeMap",
                    "mapper" :
 "org.forgerock.openam.federation.rest.schema.mappers.AttributeMapMapper"
                  },
                  "items" : {
                    "type" : "object",
                    "properties" : {
                      "nameFormatUri" : {
                        "title" : "Name Format Uri",
                        "propertyOrder" : 0,
                        "type" : "string"
                      },
                      "samlAttribute" : {
                        "title" : "SAML Attribute",
                        "propertyOrder" : 1,
                        "type" : "string"
                      },
                      "localAttribute" : {
                        "title" : "Local Attribute",
                        "propertyOrder" : 2,
                        "type" : "string"
                      },
                      "binary" : {
                        "title" : "Binary",
                        "propertyOrder" : 3,
                        "type" : "boolean"
                      }
                    },
                    "required" : [ "samlAttribute", "localAttribute" ]
                  }
                }
              },
              "required" : [ "attributeMapper" ]
            },
            "accountMapper" : {
              "traverseObject" : true,
              "title" : "Account Mapper",
              "type" : "object",
              "properties" : {
                "accountMapper" : {
                  "attributeKey" : "idpAccountMapper",
                  "title" : "Account Mapper",
                  "type" : "string",
                  "default" : "com.sun.identity.saml2.plugins.DefaultIDPAccountMapper",
                  "description" : "Used to generate Name Identifier in Single Sign-on assertion and
 find user's identity from incoming request."
                },
                "disableNameIdPersistence" : {
                  "attributeKey" : "idpDisableNameIDPersistence",
                  "title" : "Disable NameID Persistence",
                  "type" : "boolean",
```

```
                "description" : "Disables the persistence of the NameID values into the User Data
Store for all persistent NameID-Formats. When the persistent NameID-Format is in use, disabling
NameID persistence is not recommended. Note that by preventing the storage of the NameID values,
the ManageNameID and the NameIDMapping SAML profiles will no longer work when using any persistent
NameID-Formats. Existing account links that have been established (and persisted) previously, will
not be removed when enabling this feature.",
                "default" : false
              }
            }
          },
          "localConfiguration" : {
            "traverseObject" : true,
            "title" : "Local Configuration",
            "type" : "object",
            "properties" : {
              "authUrl" : {
                "attributeKey" : "AuthUrl",
                "type" : "string",
                "title" : "Auth URL",
                "description" : "URL to redirect for user authentication if required"
              },
              "reverseProxyUrl" : {
                "attributeKey" : "RpUrl",
                "type" : "string",
                "title" : "Reverse Proxy URL",
                "description" : "URL of the Reverse Proxy where the SAML endpoints are available"
              },
              "externalApplicationLogoutUrl" : {
                "attributeKey" : "appLogoutUrl",
                "type" : "string",
                "title" : "External Application Logout URL",
                "description" : "This is the logout URL for an external application. Once the server
receives logout request from the remote partner, a request will be sent to the logout URL using back
channel HTTP POST with all cookies. Optionally, a user session property could be sent as HTTP header
and POST parameter if a query parameter \"appsessionproperty\" (set to the session property name) is
included in the URL. e.g. \"http://www.app.domain.com/uri/logout?appsessionproperty=mail\"."
              }
            }
          }
        }
      },
      "services" : {
        "propertyOrder" : 2,
        "title" : "Services",
        "type" : "object",
        "traverseObject" : true,
        "properties" : {
          "metaAlias" : {
            "attributeKey" : "metaAlias",
            "default" : "{idpMetaAlias}",
            "type" : "string",
            "title" : "Meta Alias",
            "readOnly" : true,
            "description" : "The Meta Alias attribute is specific to providers using OpenAM
therefore, a null value for a remote provider configuration is possible."
          },
          "serviceAttributes" : {
            "title" : "IDP Service Attributes",
            "type" : "object",
```

```
              "traverseObject" : true,
              "properties" : {
                "artifactResolutionService" : {
                  "title" : "Artifact Resolution Service",
                  "type" : "array",
                  "attributePath" : {
                    "value" : "artifactResolutionService",
                    "mapper" :
"org.forgerock.openam.federation.rest.schema.mappers.IndexedEndpointMapper"
                  },
                  "items" : {
                    "type" : "object",
                    "properties" : {
                      "binding" : {
                        "title" : "Binding",
                        "anyOf" : [ {
                          "title" : "Predefined Binding",
                          "type" : "string",
                          "enum" : [ "urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect",
"urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST", "urn:oasis:names:tc:SAML:2.0:bindings:SOAP",
"urn:oasis:names:tc:SAML:2.0:bindings:PAOS" ],
                          "enumNames" : [ "HTTP-REDIRECT", "HTTP-POST", "SOAP", "PAOS" ]
                        }, {
                          "title" : "Custom Binding",
                          "type" : "string"
                        } ]
                      },
                      "location" : {
                        "title" : "Location",
                        "type" : "string"
                      },
                      "responseLocation" : {
                        "title" : "Response Location",
                        "type" : "string"
                      }
                    },
                    "required" : [ "location" ]
                  },
                  "default" : [ {
                    "binding" : "urn:oasis:names:tc:SAML:2.0:bindings:SOAP",
                    "location" : "{baseUrl}/ArtifactResolver/metaAlias{idpMetaAlias}"
                  } ]
                },
                "singleLogoutService" : {
                  "title" : "Single Logout Service",
                  "type" : "array",
                  "attributePath" : {
                    "value" : "singleLogoutService",
                    "mapper" : "org.forgerock.openam.federation.rest.schema.mappers.EndpointMapper"
                  },
                  "items" : {
                    "type" : "object",
                    "properties" : {
                      "binding" : {
                        "title" : "Binding",
                        "anyOf" : [ {
                          "title" : "Predefined Binding",
                          "type" : "string",
```

```
                        "enum" : [ "urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect",
"urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST", "urn:oasis:names:tc:SAML:2.0:bindings:SOAP",
"urn:oasis:names:tc:SAML:2.0:bindings:PAOS" ],
                        "enumNames" : [ "HTTP-REDIRECT", "HTTP-POST", "SOAP", "PAOS" ]
                      }, {
                        "title" : "Custom Binding",
                        "type" : "string"
                      } ]
                    },
                    "location" : {
                      "title" : "Location",
                      "type" : "string"
                    },
                    "responseLocation" : {
                      "title" : "Response Location",
                      "type" : "string"
                    }
                  },
                  "required" : [ "location" ]
                },
                "default" : [ {
                  "binding" : "urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect",
                  "location" : "{baseUrl}/IDPSloRedirect/metaAlias{idpMetaAlias}",
                  "responseLocation" : "{baseUrl}/IDPSloRedirect/metaAlias{idpMetaAlias}"
                }, {
                  "binding" : "urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST",
                  "location" : "{baseUrl}/IDPSloPOST/metaAlias{idpMetaAlias}",
                  "responseLocation" : "{baseUrl}/IDPSloPOST/metaAlias{idpMetaAlias}"
                }, {
                  "binding" : "urn:oasis:names:tc:SAML:2.0:bindings:SOAP",
                  "location" : "{baseUrl}/IDPSloSoap/metaAlias{idpMetaAlias}"
                } ]
              },
              "nameIdService" : {
                "title" : "Manage NameID Service",
                "type" : "array",
                "attributePath" : {
                  "value" : "manageNameIDService",
                  "mapper" : "org.forgerock.openam.federation.rest.schema.mappers.EndpointMapper"
                },
                "items" : {
                  "type" : "object",
                  "properties" : {
                    "binding" : {
                      "title" : "Binding",
                      "anyOf" : [ {
                        "title" : "Predefined Binding",
                        "type" : "string",
                        "enum" : [ "urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect",
"urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST", "urn:oasis:names:tc:SAML:2.0:bindings:SOAP",
"urn:oasis:names:tc:SAML:2.0:bindings:PAOS" ],
                        "enumNames" : [ "HTTP-REDIRECT", "HTTP-POST", "SOAP", "PAOS" ]
                      }, {
                        "title" : "Custom Binding",
                        "type" : "string"
                      } ]
                    },
                    "location" : {
                      "title" : "Location",
```

```
                      "type" : "string"
                    },
                    "responseLocation" : {
                      "title" : "Response Location",
                      "type" : "string"
                    }
                  },
                  "required" : [ "location" ]
                },
                "default" : [ {
                  "binding" : "urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect",
                  "location" : "{baseUrl}/IDPMniRedirect/metaAlias{idpMetaAlias}",
                  "responseLocation" : "{baseUrl}/IDPMniRedirect/metaAlias{idpMetaAlias}"
                }, {
                  "binding" : "urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST",
                  "location" : "{baseUrl}/IDPMniPOST/metaAlias{idpMetaAlias}",
                  "responseLocation" : "{baseUrl}/IDPMniPOST/metaAlias{idpMetaAlias}"
                }, {
                  "binding" : "urn:oasis:names:tc:SAML:2.0:bindings:SOAP",
                  "location" : "{baseUrl}/IDPMniSoap/metaAlias{idpMetaAlias}"
                } ]
              },
              "singleSignOnService" : {
                "title" : "Single SignOn Service",
                "type" : "array",
                "attributePath" : {
                  "value" : "singleSignOnService",
                  "mapper" : "org.forgerock.openam.federation.rest.schema.mappers.EndpointMapper"
                },
                "items" : {
                  "type" : "object",
                  "properties" : {
                    "binding" : {
                      "title" : "Binding",
                      "anyOf" : [ {
                        "title" : "Predefined Binding",
                        "type" : "string",
                        "enum" : [ "urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect",
"urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST", "urn:oasis:names:tc:SAML:2.0:bindings:SOAP",
"urn:oasis:names:tc:SAML:2.0:bindings:PAOS" ],
                        "enumNames" : [ "HTTP-REDIRECT", "HTTP-POST", "SOAP", "PAOS" ]
                      }, {
                        "title" : "Custom Binding",
                        "type" : "string"
                      } ]
                    },
                    "location" : {
                      "title" : "Location",
                      "type" : "string"
                    },
                    "responseLocation" : {
                      "title" : "Response Location",
                      "type" : "string"
                    }
                  },
                  "required" : [ "location" ]
                },
                "default" : [ {
                  "binding" : "urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect",
```

```
                    "location" : "{baseUrl}/SSORedirect/metaAlias{idpMetaAlias}"
                  }, {
                    "binding" : "urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST",
                    "location" : "{baseUrl}/SSOPOST/metaAlias{idpMetaAlias}"
                  }, {
                    "binding" : "urn:oasis:names:tc:SAML:2.0:bindings:SOAP",
                    "location" : "{baseUrl}/SSOSoap/metaAlias{idpMetaAlias}"
                  } ]
                }
              }
            },
            "nameIdMapping" : {
              "title" : "NameID Mapping",
              "type" : "array",
              "attributePath" : {
                "value" : "nameIDMappingService",
                "mapper" : "org.forgerock.openam.federation.rest.schema.mappers.EndpointMapper"
              },
              "items" : {
                "type" : "object",
                "properties" : {
                  "binding" : {
                    "title" : "Binding",
                    "anyOf" : [ {
                      "title" : "Predefined Binding",
                      "type" : "string",
                      "enum" : [ "urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect",
"urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST", "urn:oasis:names:tc:SAML:2.0:bindings:SOAP",
"urn:oasis:names:tc:SAML:2.0:bindings:PAOS" ],
                      "enumNames" : [ "HTTP-REDIRECT", "HTTP-POST", "SOAP", "PAOS" ]
                    }, {
                      "title" : "Custom Binding",
                      "type" : "string"
                    } ]
                  },
                  "location" : {
                    "title" : "Location",
                    "type" : "string"
                  },
                  "responseLocation" : {
                    "title" : "Response Location",
                    "type" : "string"
                  }
                },
                "required" : [ "location" ]
              },
              "default" : [ {
                "binding" : "urn:oasis:names:tc:SAML:2.0:bindings:SOAP",
                "location" : "{baseUrl}/NIMSoap/metaAlias{idpMetaAlias}"
              } ]
            },
            "assertionIdRequest" : {
              "title" : "Assertion ID Request Service",
              "type" : "array",
              "attributePath" : {
                "value" : "assertionIDRequestService",
                "mapper" : "org.forgerock.openam.federation.rest.schema.mappers.EndpointMapper"
              },
              "items" : {
```

```
                "type" : "object",
                "properties" : {
                  "binding" : {
                    "title" : "Binding",
                    "anyOf" : [ {
                      "title" : "Predefined Binding",
                      "type" : "string",
                      "enum" : [ "urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect",
"urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST", "urn:oasis:names:tc:SAML:2.0:bindings:SOAP",
"urn:oasis:names:tc:SAML:2.0:bindings:PAOS" ],
                      "enumNames" : [ "HTTP-REDIRECT", "HTTP-POST", "SOAP", "PAOS" ]
                    }, {
                      "title" : "Custom Binding",
                      "type" : "string"
                    } ]
                  },
                  "location" : {
                    "title" : "Location",
                    "type" : "string"
                  },
                  "responseLocation" : {
                    "title" : "Response Location",
                    "type" : "string"
                  }
                },
                "required" : [ "location" ]
              },
              "default" : [ {
                "binding" : "urn:oasis:names:tc:SAML:2.0:bindings:SOAP",
                "location" : "{baseUrl}/AIDReqSoap/IDPRole/metaAlias{idpMetaAlias}"
              }, {
                "binding" : "urn:oasis:names:tc:SAML:2.0:bindings:URI",
                "location" : "{baseUrl}/AIDReqUri/IDPRole/metaAlias{idpMetaAlias}"
              } ]
            }
          },
          "required" : [ "metaAlias" ]
        },
        "advanced" : {
          "traverseObject" : true,
          "propertyOrder" : 3,
          "title" : "Advanced",
          "type" : "object",
          "properties" : {
            "saeConfiguration" : {
              "traverseObject" : true,
              "title" : "SAE Configuration",
              "type" : "object",
              "properties" : {
                "idpUrl" : {
                  "attributeKey" : "saeIDPUrl",
                  "title" : "IDP URL",
                  "description" : "URL endpoint on the Identity Provider that can handle SAE
requests.",
                  "type" : "string",
                  "default" : "{baseUrl}/idpsaehandler/metaAlias{idpMetaAlias}"
                },
                "applicationSecurityConfiguration" : {
                  "attributeKey" : {
```

```
                    "value" : "saeAppSecretList",
                    "mapper" :
"org.forgerock.openam.federation.rest.schema.mappers.ApplicationSecurityConfigItemMapper"
                  },
                  "title" : "Application Security Configuration",
                  "type" : "array",
                  "items" : {
                    "type" : "object",
                    "properties" : {
                      "url" : {
                        "title" : "URL",
                        "propertyOrder" : 0,
                        "type" : "string"
                      },
                      "type" : {
                        "title" : "Type",
                        "propertyOrder" : 1,
                        "type" : "string"
                      },
                      "pubKeyAlias" : {
                        "title" : "Public Key Alias",
                        "propertyOrder" : 2,
                        "type" : "string"
                      },
                      "encryptionAlgorithm" : {
                        "title" : "Encryption Algorithm",
                        "propertyOrder" : 3,
                        "type" : "string"
                      },
                      "encryptionKeyStrength" : {
                        "title" : "Encryption Key Strength",
                        "propertyOrder" : 4,
                        "type" : "string"
                      },
                      "secret" : {
                        "title" : "Secret",
                        "propertyOrder" : 5,
                        "type" : "string"
                      }
                    },
                    "required" : [ "url", "secret" ]
                  }
                }
              }
            },
            "ecpConfiguration" : {
              "traverseObject" : true,
              "title" : "ECP Configuration",
              "type" : "object",
              "properties" : {
                "idpSessionMapper" : {
                  "attributeKey" : "idpECPSessionMapper",
                  "title" : "IDP Session Mapper",
                  "description" : "Defines an implementation class for the session mapper SPI. The
mapper finds a valid session from HTTP servlet request on IDP with ECP profile.",
                  "type" : "string",
                  "default" : "com.sun.identity.saml2.plugins.DefaultIDPECPSessionMapper"
                }
              }
```

```
          },
          "sessionSynchronization" : {
            "traverseObject" : true,
            "title" : "Session Synchronization",
            "type" : "object",
            "properties" : {
              "enabled" : {
                "attributeKey" : "idpSessionSyncEnabled",
                "title" : "Enabled",
                "description" : "If this is enabled, when a session times out, the Identity Provider
notifies all Service Providers to log out. A session may time out, for example, when max-idle time or
max-session time is reached.",
                "type" : "boolean",
                "default" : false
              }
            }
          },
          "idpFinderImplementation" : {
            "traverseObject" : true,
            "title" : "IDP Finder Implementation",
            "type" : "object",
            "properties" : {
              "idpFinderImplementationClass" : {
                "attributeKey" : "proxyIDPFinderClass",
                "title" : "IDP Finder implementation class",
                "description" : "Defines an implementation class for the Proxy IDP Finder SPI. The
implementation is used to find a preferred IdP to send the proxied Authentication Request",
                "type" : "string"
              },
              "idpFinderJsp" : {
                "attributeKey" : "proxyIDPFinderJSP",
                "title" : "IdP Finder JSP",
                "description" : "Specify the JSP that will present the IdP List to the user, if
required by the class implementation (example: proxyidpfinder.jsp)",
                "type" : "string"
              },
              "enableProxyIdpFinderForAllSps" : {
                "attributeKey" : "enableProxyIDPFinderForAllSPs",
                "title" : "Enable Proxy IDP Finder for all SPs",
                "description" : "If this is enabled the proxy idp finder will be enabled for all the
remote SPs regardless of what they have configured in their extended metadata",
                "type" : "boolean",
                "default" : false
              }
            }
          },
          "relayStateUrlList" : {
            "traverseObject" : true,
            "title" : "Relay State URL List",
            "type" : "object",
            "properties" : {
              "relayStateUrlList" : {
                "attributeKey" : "relayStateUrlList",
                "title" : "Relay State URL List",
                "type" : "array",
                "items" : {
                  "type" : "string"
                }
              }
```

```
            }
          },
          "idpAdapter" : {
            "traverseObject" : true,
            "title" : "IDP Adapter",
            "type" : "object",
            "properties" : {
              "idpAdapterClass" : {
                "attributeKey" : "idpAdapter",
                "title" : "IDP Adapter Class",
                "type" : "string"
              }
            }
          }
        }
      }
    },
    "serviceProvider" : {
      "title" : "Service Provider",
      "description" : "This schema describes a SAML2 service provider.",
      "type" : "object",
      "traverseObject" : true,
      "properties" : {
        "assertionContent" : {
          "propertyOrder" : 0,
          "traverseObject" : true,
          "title" : "Assertion Content",
          "type" : "object",
          "properties" : {
            "signingAndEncryption" : {
              "traverseObject" : true,
              "title" : "Signing And Encryption",
              "type" : "object",
              "properties" : {
                "requestResponseSigning" : {
                  "traverseObject" : true,
                  "description" : "Select the checkbox for each request/response that should be signed
\n",
                  "title" : "Request/Response Signing",
                  "type" : "object",
                  "properties" : {
                    "authenticationRequest" : {
                      "attributePath" : {
                        "value" : "/authnRequestsSigned"
                      },
                      "title" : "Authentication Requests Signed",
                      "type" : "boolean",
                      "default" : false
                    },
                    "assertion" : {
                      "attributePath" : "/wantAssertionsSigned",
                      "title" : "Assertions Signed",
                      "type" : "boolean",
                      "default" : false
                    },
                    "postResponse" : {
                      "attributeKey" : "wantPOSTResponseSigned",
                      "title" : "POST Response Signed",
```

```
                "type" : "boolean",
                "default" : false
              },
              "artifactResponse" : {
                "attributeKey" : "wantArtifactResponseSigned",
                "title" : "Artifact Response Signed",
                "type" : "boolean",
                "default" : false
              },
              "logoutRequest" : {
                "attributeKey" : "wantLogoutRequestSigned",
                "title" : "Logout Request Signed",
                "type" : "boolean",
                "default" : false
              },
              "logoutResponse" : {
                "attributeKey" : "wantLogoutResponseSigned",
                "title" : "Logout Response Signed",
                "type" : "boolean",
                "default" : false
              },
              "manageNameIdRequest" : {
                "attributeKey" : "wantMNIRequestSigned",
                "title" : "Manage NameID Request Signed",
                "type" : "boolean",
                "default" : false
              },
              "manageNameIdResponse" : {
                "attributeKey" : "wantMNIResponseSigned",
                "title" : "Manage NameID Response Signed",
                "type" : "boolean",
                "default" : false
              }
            }
          },
          "encryption" : {
            "traverseObject" : true,
            "title" : "Encryption",
            "type" : "object",
            "properties" : {
              "attributeEncryption" : {
                "attributeKey" : "wantAttributeEncrypted",
                "title" : "Attribute Encryption",
                "type" : "boolean"
              },
              "assertionEncryption" : {
                "attributeKey" : "wantAssertionEncrypted",
                "title" : "Assertion Encryption",
                "type" : "boolean"
              },
              "nameIdEncryption" : {
                "attributeKey" : "wantNameIDEncrypted",
                "title" : "NameID Encryption",
                "type" : "boolean"
              }
            }
          },
          "secretIdAndAlgorithms" : {
            "traverseObject" : true,
```

```
                  "title" : "Secret ID And Algorithms",
                  "type" : "object",
                  "properties" : {
                    "secretIdIdentifier" : {
                      "type" : "string",
                      "attributeKey" : "secretIdIdentifier",
                      "title" : "Secret ID Identifier",
                      "description" : "This identifier determines the secret ID for this
 entity provider when resolving secrets. For example when this value is set to \"demo\", the
 entity provider will use am.applications.federation.entity.providers.saml2.demo.signing and
 am.applications.federation.entity.providers.saml2.demo.encryption secret IDs to resolve the signing
 and encryption secrets. When left unspecified, AM will use the entity provider role (service
 provider, identity provider, etc.) specific default global secret IDs. When the secret ID identifier
 for a given role is modified, the corresponding mapping is removed if it isnâ##t referenced by other
 entities."
                    },
                    "signingAlgorithm" : {
                      "title" : "Signing Algorithm",
                      "type" : "array",
                      "attributePath" : {
                        "value" : "extensions",
                        "mapper" :
 "org.forgerock.openam.federation.rest.schema.mappers.SigningAlgorithmMapper"
                      },
                      "items" : {
                        "type" : "string",
                        "enum" : [ "http://www.w3.org/2000/09/xmldsig#rsa-sha1", "http://
www.w3.org/2001/04/xmldsig-more#ecdsa-sha256", "http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha384",
 "http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha512", "http://www.w3.org/2001/04/xmldsig-more#rsa-
sha256", "http://www.w3.org/2001/04/xmldsig-more#rsa-sha384", "http://www.w3.org/2001/04/xmldsig-
more#rsa-sha512", "http://www.w3.org/2009/xmldsig11#dsa-sha256" ],
                        "enumNames" : [ "http://www.w3.org/2000/09/xmldsig#rsa-sha1", "http://
www.w3.org/2001/04/xmldsig-more#ecdsa-sha256", "http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha384",
 "http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha512", "http://www.w3.org/2001/04/xmldsig-more#rsa-
sha256", "http://www.w3.org/2001/04/xmldsig-more#rsa-sha384", "http://www.w3.org/2001/04/xmldsig-
more#rsa-sha512", "http://www.w3.org/2009/xmldsig11#dsa-sha256" ]
                      }
                    },
                    "digestAlgorithm" : {
                      "title" : "Digest Algorithm",
                      "type" : "array",
                      "attributePath" : {
                        "value" : "extensions",
                        "mapper" :
 "org.forgerock.openam.federation.rest.schema.mappers.DigestAlgorithmMapper"
                      },
                      "items" : {
                        "type" : "string",
                        "enum" : [ "http://www.w3.org/2000/09/xmldsig#sha1", "http://
www.w3.org/2001/04/xmldsig-more#sha384", "http://www.w3.org/2001/04/xmlenc#sha256", "http://
www.w3.org/2001/04/xmlenc#sha512", "http://www.w3.org/2007/05/xmldsig-more#sha3-256", "http://
www.w3.org/2007/05/xmldsig-more#sha3-384", "http://www.w3.org/2007/05/xmldsig-more#sha3-512" ],
                        "enumNames" : [ "http://www.w3.org/2000/09/xmldsig#sha1", "http://
www.w3.org/2001/04/xmldsig-more#sha384", "http://www.w3.org/2001/04/xmlenc#sha256", "http://
www.w3.org/2001/04/xmlenc#sha512", "http://www.w3.org/2007/05/xmldsig-more#sha3-256", "http://
www.w3.org/2007/05/xmldsig-more#sha3-384", "http://www.w3.org/2007/05/xmldsig-more#sha3-512" ]
                      }
                    },
                    "encryptionAlgorithm" : {
```

```
                    "title" : "Encryption Algorithm",
                    "type" : "array",
                    "attributeKey" : {
                      "value" : "encryptionAlgorithms",
                      "mapper" :
 "org.forgerock.openam.federation.rest.schema.mappers.EncryptionAlgorithmMapper"
                    },
                    "items" : {
                      "type" : "string",
                      "enum" : [ "http://www.w3.org/2009/xmlenc11#aes128-gcm", "http://
www.w3.org/2009/xmlenc11#aes192-gcm", "http://www.w3.org/2009/xmlenc11#aes256-gcm", "http://
www.w3.org/2001/04/xmlenc#aes128-cbc", "http://www.w3.org/2001/04/xmlenc#aes192-cbc", "http://
www.w3.org/2001/04/xmlenc#aes256-cbc", "http://www.w3.org/2001/04/xmlenc#rsa-1_5", "http://
www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p", "http://www.w3.org/2009/xmlenc11#rsa-oaep" ],
                      "enumNames" : [ "http://www.w3.org/2009/xmlenc11#aes128-gcm", "http://
www.w3.org/2009/xmlenc11#aes192-gcm", "http://www.w3.org/2009/xmlenc11#aes256-gcm", "http://
www.w3.org/2001/04/xmlenc#aes128-cbc", "http://www.w3.org/2001/04/xmlenc#aes192-cbc", "http://
www.w3.org/2001/04/xmlenc#aes256-cbc", "http://www.w3.org/2001/04/xmlenc#rsa-1_5", "http://
www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p", "http://www.w3.org/2009/xmlenc11#rsa-oaep" ]
                    }
                  }
                }
              }
            },
            "nameIdFormat" : {
              "traverseObject" : true,
              "title" : "NameID Format",
              "type" : "object",
              "properties" : {
                "nameIdFormatList" : {
                  "description" : "List of NameID formats the requestor will use to contact. Order
 listed shows the order of preference",
                  "title" : "NameID Format List",
                  "attributePath" : {
                    "value" : "/nameIDFormat"
                  },
                  "type" : "array",
                  "items" : {
                    "type" : "string"
                  },
                  "default" : [ "urn:oasis:names:tc:SAML:2.0:nameid-format:persistent",
 "urn:oasis:names:tc:SAML:2.0:nameid-format:transient", "urn:oasis:names:tc:SAML:1.1:nameid-
format:emailAddress", "urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified",
 "urn:oasis:names:tc:SAML:1.1:nameid-format:WindowsDomainQualifiedName",
 "urn:oasis:names:tc:SAML:2.0:nameid-format:kerberos", "urn:oasis:names:tc:SAML:1.1:nameid-
format:X509SubjectName" ]
                },
                "disableNameIdPersistence" : {
                  "attributeKey" : "spDoNotWriteFederationInfo",
                  "title" : "Disable NameID persistence",
                  "description" : "Instructs the SP to not persist the SAML NameID into the User
 Data Store even if the NameID Format is urn:oasis:names:tc:SAML:2.0:nameid-format:persistent in the
 received Assertion and the Account Mapper has identified the local user. When local authentication
 is utilized for account linking purposes, enabling this feature will require end-users to locally
 authenticate for each SAML-based login.",
                  "type" : "boolean",
                  "default" : false
                }
```

```
            }
          },
          "authenticationContext" : {
            "traverseObject" : true,
            "title" : "Authentication Context",
            "type" : "object",
            "properties" : {
              "authenticationContextMapper" : {
                "attributeKey" : "spAuthncontextMapper",
                "title" : "Mapper",
                "type" : "string",
                "default" : "com.sun.identity.saml2.plugins.DefaultSPAuthnContextMapper"
              },
              "authContextItems" : {
                "attributeKey" : {
                  "value" : "spAuthncontextClassrefMapping",
                  "mapper" :
"org.forgerock.openam.federation.rest.schema.mappers.SpAuthContextMapper"
                },
                "description" : "Defines mapping between IDP authentication context reference and
authentication level to be set on SP side session",
                "title" : "Authentication Context",
                "type" : "array",
                "items" : {
                  "type" : "object",
                  "properties" : {
                    "contextReference" : {
                      "propertyOrder" : 0,
                      "title" : "Context Reference",
                      "anyOf" : [ {
                        "title" : "Predefined Reference",
                        "type" : "string",
                        "enum" : [ "urn:oasis:names:tc:SAML:2.0:ac:classes:InternetProtocol",
"urn:oasis:names:tc:SAML:2.0:ac:classes:InternetProtocolPassword",
"urn:oasis:names:tc:SAML:2.0:ac:classes:Kerberos",
"urn:oasis:names:tc:SAML:2.0:ac:classes:MobileOneFactorUnregistered",
"urn:oasis:names:tc:SAML:2.0:ac:classes:MobileTwoFactorUnregistered",
"urn:oasis:names:tc:SAML:2.0:ac:classes:MobileOneFactorContract",
"urn:oasis:names:tc:SAML:2.0:ac:classes:MobileTwoFactorContract",
"urn:oasis:names:tc:SAML:2.0:ac:classes:Password",
"urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport",
"urn:oasis:names:tc:SAML:2.0:ac:classes:PreviousSession",
"urn:oasis:names:tc:SAML:2.0:ac:classes:X.509", "urn:oasis:names:tc:SAML:2.0:ac:classes:PGP",
"urn:oasis:names:tc:SAML:2.0:ac:classes:SPKI", "urn:oasis:names:tc:SAML:2.0:ac:classes:XMLDSig",
"urn:oasis:names:tc:SAML:2.0:ac:classes:Smartcard",
"urn:oasis:names:tc:SAML:2.0:ac:classes:SmartcardPKI",
"urn:oasis:names:tc:SAML:2.0:ac:classes:SoftwarePKI",
"urn:oasis:names:tc:SAML:2.0:ac:classes:Telephony",
"urn:oasis:names:tc:SAML:2.0:ac:classes:NomadTelephony",
"urn:oasis:names:tc:SAML:2.0:ac:classes:PersonalTelephony",
"urn:oasis:names:tc:SAML:2.0:ac:classes:AuthenticatedTelephony",
"urn:oasis:names:tc:SAML:2.0:ac:classes:SecureRemotePassword",
"urn:oasis:names:tc:SAML:2.0:ac:classes:TLSClient",
"urn:oasis:names:tc:SAML:2.0:ac:classes:TimeSyncToken", "unspecified" ],
                        "enumNames" : [ "InternetProtocol", "InternetProtocolPassword", "Kerberos",
"MobileOneFactorUnregistered", "MobileTwoFactorUnregistered", "MobileOneFactorContract",
"MobileTwoFactorContract", "Password", "PasswordProtectedTransport", "PreviousSession", "X.509",
"PGP", "SPKI", "XMLDSig", "Smartcard", "SmartcardPKI", "SoftwarePKI", "Telephony", "NomadTelephony",
```

```
"PersonalTelephony", "AuthenticatedTelephony", "SecureRemotePassword", "TLSClient", "TimeSyncToken",
"unspecified" ]
                        }, {
                          "title" : "Custom Reference",
                          "type" : "string"
                        } ]
                      },
                      "level" : {
                        "default" : 0,
                        "minimum" : 0,
                        "propertyOrder" : 1,
                        "title" : "Level",
                        "type" : "integer"
                      },
                      "defaultItem" : {
                        "propertyOrder" : 2,
                        "title" : "Default",
                        "type" : "boolean"
                      }
                    }
                  },
                  "default" : [ {
                    "contextReference" :
"urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport",
                    "level" : "0",
                    "defaultItem" : true
                  } ]
                },
                "authenticationComparisonType" : {
                  "attributeKey" : {
                    "value" : "spAuthncontextComparisonType",
                    "mapper" :
"org.forgerock.openam.federation.rest.schema.mappers.AuthComparisonTypeMapper"
                  },
                  "title" : "Comparison Type",
                  "type" : "string",
                  "enum" : [ "None", "Exact", "Minimum", "Maximum", "Better" ],
                  "default" : "Exact"
                },
                "includeRequestedAuthenticationContext" : {
                  "attributeKey" : "includeRequestedAuthnContext",
                  "title" : "Include Request Authentication Context",
                  "description" : "Enable to include the Requested Authentication Context in the
Authentication Request, enabled by default.",
                  "type" : "boolean",
                  "default" : true
                }
              }
            },
            "assertionTimeSkew" : {
              "attributeKey" : "assertionTimeSkew",
              "title" : "Assertion Time Skew",
              "description" : "Is in seconds. Skew time for NotBefore and NotOnOrAfter attributes in
assertion SubjectConfirmationData and Conditions",
              "type" : "integer",
              "default" : 300
            },
            "basicAuthentication" : {
              "traverseObject" : true,
```

```
              "description" : "Configure basic authentication setting for Soap based binding",
              "title" : "Basic Authentication",
              "type" : "object",
              "properties" : {
                "enabled" : {
                  "attributeKey" : "basicAuthOn",
                  "title" : "Enabled",
                  "type" : "boolean",
                  "default" : false
                },
                "userName" : {
                  "attributeKey" : "basicAuthUser",
                  "title" : "User Name",
                  "type" : "string"
                },
                "password" : {
                  "title" : "Password",
                  "attributeKey" : {
                    "value" : "basicAuthPassword",
                    "mapper" : "org.forgerock.openam.federation.rest.schema.mappers.PasswordMapper"
                  },
                  "type" : "string",
                  "format" : "password"
                }
              }
            }
          }
        },
        "assertionProcessing" : {
          "propertyOrder" : 1,
          "traverseObject" : true,
          "title" : "Assertion Processing",
          "type" : "object",
          "properties" : {
            "attributeMapper" : {
              "traverseObject" : true,
              "title" : "Attribute Mapper",
              "type" : "object",
              "properties" : {
                "attributeMapper" : {
                  "attributeKey" : "spAttributeMapper",
                  "title" : "Attribute Mapper",
                  "type" : "string",
                  "default" : "com.sun.identity.saml2.plugins.DefaultSPAttributeMapper"
                },
                "attributeMap" : {
                  "attributeKey" : {
                    "value" : "attributeMap",
                    "mapper" : "org.forgerock.openam.federation.rest.schema.mappers.KeyValueMapper"
                  },
                  "description" : "This mapping is the configuration used by the Attribute Mapper.
Mapping should be defined as SAML ATTRIBUTE NAME=PROFILE ATTRIBUTE NAME in assertion. Example:
EmailAddress=mail, Address=postaladdress.",
                  "title" : "Attribute Map",
                  "type" : "array",
                  "items" : {
                    "type" : "object",
                    "properties" : {
                      "key" : {
```

```
                      "propertyOrder" : 0,
                      "title" : "Key",
                      "type" : "string"
                    },
                    "value" : {
                      "propertyOrder" : 1,
                      "title" : "Value",
                      "type" : "string"
                    }
                  }
                },
                "default" : [ {
                  "key" : "*",
                  "value" : "*"
                } ]
              }
            },
            "required" : [ "attributeMapper" ]
          },
          "autoFederation" : {
            "description" : "Enable Auto Federation if not already federated",
            "traverseObject" : true,
            "title" : "Auto Federation",
            "type" : "object",
            "properties" : {
              "autoFedEnabled" : {
                "attributeKey" : "autofedEnabled",
                "title" : "Enabled",
                "description" : "Enable Auto Federation if not already federated",
                "type" : "boolean",
                "default" : false
              },
              "autoFedAttribute" : {
                "attributeKey" : "autofedAttribute",
                "title" : "Attribute",
                "description" : "This SAML attribute identifies the user to auto federate with. If
this attribute is not present in the assertion then the value of the NameID is used instead. If there
is a mapping defined for this attribute, it will be used along with the value when searching for the
local user. If the local user can not be found and Dynamic or Ignored Profile is enabled, the value
will be used as the local user's UID instead.",
                "type" : "string"
              }
            }
          },
          "accountMapping" : {
            "traverseObject" : true,
            "title" : "Account Mapper",
            "type" : "object",
            "properties" : {
              "spAccountMapper" : {
                "attributeKey" : "spAccountMapper",
                "title" : "Account Mapper",
                "description" : "Helps to find the user on local side based on incoming assertion",
                "type" : "string",
                "default" : "com.sun.identity.saml2.plugins.DefaultSPAccountMapper"
              },
              "useNameIDAsSPUserID" : {
                "attributeKey" : "useNameIDAsSPUserID",
                "title" : "Use Name ID as User ID",
```

```
                "description" : "Use value of Name ID from the incoming Assertion to find the local
user as the final resort, if other means do not apply",
                "type" : "boolean",
                "default" : false
              },
              "transientUser" : {
                "attributeKey" : "transientUser",
                "description" : "Can be null. If specified this will be the mapped SP user incase of
transient federation",
                "title" : "Transient User",
                "type" : "string"
              }
            }
          },
          "responseArtifactMessageEncoding" : {
            "traverseObject" : true,
            "title" : "Artifact Message Encoding",
            "type" : "object",
            "properties" : {
              "encoding" : {
                "attributeKey" : {
                  "value" : "responseArtifactMessageEncoding",
                  "mapper" :
"org.forgerock.openam.federation.rest.schema.mappers.MessageEncodingMapper"
                },
                "title" : "Artifact Message Encoding",
                "type" : "string",
                "enum" : [ "URI", "FORM" ],
                "default" : "URI"
              }
            }
          },
          "url" : {
            "traverseObject" : true,
            "title" : "URL",
            "type" : "object",
            "properties" : {
              "localAuthUrl" : {
                "attributeKey" : "localAuthURL",
                "title" : "Local Authentication Url",
                "description" : "For local authentication",
                "type" : "string"
              },
              "intermediateUrl" : {
                "attributeKey" : "intermediateUrl",
                "title" : "Intermediate Url",
                "description" : "This is the intermediate point that SP will redirect to before the
final relay state",
                "type" : "string"
              },
              "appLogoutUrl" : {
                "attributeKey" : "appLogoutUrl",
                "title" : "External Application Logout URL",
                "description" : "This is the logout URL for an external application. Once the server
receives logout request from the remote partner, a request will be sent to the logout URL using back
channel HTTP POST with all cookies. Optionally, a user session property could be sent as HTTP header
and POST parameter if a query parameter \"appsessionproperty\" (set to the session property name) is
included in the URL. e.g. \"http://www.app.domain.com/uri/logout?appsessionproperty=mail\"",
                "type" : "string"
```

```
              }
            }
          },
          "defaultRelayState" : {
            "attributeKey" : "defaultRelayState",
            "title" : "Default Relay State Url",
            "description" : "This is the default relay state URL that the SP will redirect to, in
case there is no relay state specified in the response",
            "type" : "string"
          },
          "adapter" : {
            "traverseObject" : true,
            "title" : "Adapter",
            "type" : "object",
            "properties" : {
              "spAdapter" : {
                "attributeKey" : "spAdapter",
                "title" : "Adapter",
                "description" : "Implementation class for the SAML2ServiceProviderAdapter which is
used to add application specific processing logic during federation process",
                "type" : "string"
              },
              "spAdapterEnv" : {
                "attributeKey" : {
                  "value" : "spAdapterEnv",
                  "mapper" : "org.forgerock.openam.federation.rest.schema.mappers.KeyValueMapper"
                },
                "title" : "Adapter Environment",
                "type" : "array",
                "items" : {
                  "type" : "object",
                  "properties" : {
                    "key" : {
                      "propertyOrder" : 0,
                      "title" : "Key",
                      "type" : "string"
                    },
                    "value" : {
                      "propertyOrder" : 1,
                      "title" : "Value",
                      "type" : "string"
                    }
                  }
                }
              }
            }
          }
        },
        "services" : {
          "propertyOrder" : 2,
          "traverseObject" : true,
          "type" : "object",
          "title" : "Services",
          "properties" : {
            "metaAlias" : {
              "attributeKey" : "metaAlias",
              "default" : "{spMetaAlias}",
              "title" : "MetaAlias",
```

```
              "description" : "The MetaAlias attribute is specific to providers using OpenAM
therefore, a null value for a remote provider configuration is possible.",
              "type" : "string",
              "readOnly" : true
            },
            "serviceAttributes" : {
              "traverseObject" : true,
              "title" : "SP Service Attributes",
              "type" : "object",
              "properties" : {
                "singleLogoutService" : {
                  "title" : "Single Logout Service",
                  "type" : "array",
                  "attributePath" : {
                    "value" : "singleLogoutService",
                    "mapper" : "org.forgerock.openam.federation.rest.schema.mappers.EndpointMapper"
                  },
                  "items" : {
                    "type" : "object",
                    "properties" : {
                      "binding" : {
                        "title" : "Binding",
                        "anyOf" : [ {
                          "title" : "Predefined Binding",
                          "type" : "string",
                          "enum" : [ "urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect",
"urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST", "urn:oasis:names:tc:SAML:2.0:bindings:SOAP",
"urn:oasis:names:tc:SAML:2.0:bindings:PAOS" ],
                          "enumNames" : [ "HTTP-REDIRECT", "HTTP-POST", "SOAP", "PAOS" ]
                        }, {
                          "title" : "Custom Binding",
                          "type" : "string"
                        } ]
                      },
                      "location" : {
                        "title" : "Location",
                        "type" : "string"
                      },
                      "responseLocation" : {
                        "title" : "Response Location",
                        "type" : "string"
                      }
                    },
                    "required" : [ "location" ]
                  },
                  "default" : [ {
                    "binding" : "urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect",
                    "location" : "{baseUrl}/SPSloRedirect/metaAlias{spMetaAlias}",
                    "responseLocation" : "{baseUrl}/SPSloRedirect/metaAlias{spMetaAlias}"
                  }, {
                    "binding" : "urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST",
                    "location" : "{baseUrl}/SPSloPOST/metaAlias{spMetaAlias}",
                    "responseLocation" : "{baseUrl}/SPSloPOST/metaAlias{spMetaAlias}"
                  }, {
                    "binding" : "urn:oasis:names:tc:SAML:2.0:bindings:SOAP",
                    "location" : "{baseUrl}/SPSloSoap/metaAlias{spMetaAlias}"
                  } ]
                },
                "nameIdService" : {
```

```
                "title" : "Manage NameID Service",
                "type" : "array",
                "attributePath" : {
                  "value" : "manageNameIDService",
                  "mapper" : "org.forgerock.openam.federation.rest.schema.mappers.EndpointMapper"
                },
                "items" : {
                  "type" : "object",
                  "properties" : {
                    "binding" : {
                      "title" : "Binding",
                      "anyOf" : [ {
                        "title" : "Predefined Binding",
                        "type" : "string",
                        "enum" : [ "urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect",
"urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST", "urn:oasis:names:tc:SAML:2.0:bindings:SOAP",
"urn:oasis:names:tc:SAML:2.0:bindings:PAOS" ],
                        "enumNames" : [ "HTTP-REDIRECT", "HTTP-POST", "SOAP", "PAOS" ]
                      }, {
                        "title" : "Custom Binding",
                        "type" : "string"
                      } ]
                    },
                    "location" : {
                      "title" : "Location",
                      "type" : "string"
                    },
                    "responseLocation" : {
                      "title" : "Response Location",
                      "type" : "string"
                    }
                  },
                  "required" : [ "location" ]
                },
                "default" : [ {
                  "binding" : "urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect",
                  "location" : "{baseUrl}/SPMniRedirect/metaAlias{spMetaAlias}",
                  "responseLocation" : "{baseUrl}/SPMniRedirect/metaAlias{spMetaAlias}"
                }, {
                  "binding" : "urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST",
                  "location" : "{baseUrl}/SPMniPOST/metaAlias{spMetaAlias}",
                  "responseLocation" : "{baseUrl}/SPMniPOST/metaAlias{spMetaAlias}"
                }, {
                  "binding" : "urn:oasis:names:tc:SAML:2.0:bindings:SOAP",
                  "location" : "{baseUrl}/SPMniSoap/metaAlias{spMetaAlias}",
                  "responseLocation" : "{baseUrl}/SPMniSoap/metaAlias{spMetaAlias}"
                } ]
              },
              "assertionConsumerService" : {
                "attributePath" : {
                  "value" : "assertionConsumerService",
                  "mapper" :
"org.forgerock.openam.federation.rest.schema.mappers.ExtendedIndexedEndpointMapper"
                },
                "title" : "Assertion Consumer Service",
                "description" : "Location denotes the URL to accept the respective request type.
Index denotes the index of the URL in the standard metadata",
                "type" : "array",
                "items" : {
```

```
                    "type" : "object",
                    "properties" : {
                      "isDefault" : {
                        "type" : "boolean"
                      },
                      "binding" : {
                        "title" : "Binding",
                        "anyOf" : [ {
                          "title" : "Predefined Binding",
                          "type" : "string",
                          "enum" : [ "urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Artifact",
"urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST", "urn:oasis:names:tc:SAML:2.0:bindings:PAOS" ],
                          "enumNames" : [ "HTTP-Artifact", "HTTP-POST", "PAOS" ]
                        }, {
                          "title" : "Custom Binding",
                          "type" : "string"
                        } ]
                      },
                      "location" : {
                        "title" : "Location",
                        "type" : "string"
                      },
                      "index" : {
                        "type" : "integer"
                      }
                    }
                  },
                  "default" : [ {
                    "isDefault" : true,
                    "binding" : "urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Artifact",
                    "location" : "{baseUrl}/Consumer/metaAlias{spMetaAlias}",
                    "index" : "0"
                  }, {
                    "isDefault" : false,
                    "binding" : "urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST",
                    "location" : "{baseUrl}/Consumer/metaAlias{spMetaAlias}",
                    "index" : "1"
                  }, {
                    "isDefault" : false,
                    "binding" : "urn:oasis:names:tc:SAML:2.0:bindings:PAOS",
                    "location" : "{baseUrl}/Consumer/ECP/metaAlias{spMetaAlias}",
                    "index" : "2"
                  } ]
                }
              }
            }
          }
        },
        "advanced" : {
          "propertyOrder" : 3,
          "traverseObject" : true,
          "type" : "object",
          "title" : "Advanced",
          "properties" : {
            "saeConfiguration" : {
              "traverseObject" : true,
              "title" : "SAE Configuration",
              "type" : "object",
              "properties" : {
```

```
                "spUrl" : {
                  "attributeKey" : "saeSPUrl",
                  "title" : "SP URL",
                  "description" : "URL endpoint on Service Provider that can handle SAE requests.
If this URL is empty (not configured), SAE single sign-on will not be enabled. Normal samlv2 single
sign-on response will be sent to SP",
                  "type" : "string",
                  "default" : "{baseUrl}/spsaehandler/metaAlias{spMetaAlias}"
                },
                "spLogoutUrl" : {
                  "attributeKey" : "saeSPLogoutUrl",
                  "title" : "SP Logout URL",
                  "description" : "URL endpoint on the Service Provider that can handle SAE global
logout requests",
                  "type" : "string"
                },
                "applicationSecurityConfiguration" : {
                  "attributeKey" : {
                    "value" : "saeAppSecretList",
                    "mapper" :
"org.forgerock.openam.federation.rest.schema.mappers.ApplicationSecurityConfigItemMapper"
                  },
                  "title" : "Application Security Configuration",
                  "type" : "array",
                  "items" : {
                    "type" : "object",
                    "properties" : {
                      "url" : {
                        "title" : "URL",
                        "propertyOrder" : 0,
                        "type" : "string"
                      },
                      "type" : {
                        "title" : "Type",
                        "propertyOrder" : 1,
                        "type" : "string"
                      },
                      "pubKeyAlias" : {
                        "title" : "Public Key Alias",
                        "propertyOrder" : 2,
                        "type" : "string"
                      },
                      "encryptionAlgorithm" : {
                        "title" : "Encryption Algorithm",
                        "propertyOrder" : 3,
                        "type" : "string"
                      },
                      "encryptionKeyStrength" : {
                        "title" : "Encryption Key Strength",
                        "propertyOrder" : 4,
                        "type" : "string"
                      },
                      "secret" : {
                        "title" : "Secret",
                        "propertyOrder" : 5,
                        "type" : "string"
                      }
                    },
                    "required" : [ "url", "secret" ]
```

```
                }
              }
            }
          },
          "ecpConfiguration" : {
            "traverseObject" : true,
            "title" : "ECP Configuration",
            "type" : "object",
            "properties" : {
              "ecpRequestIdpListFinderImpl" : {
                "attributeKey" : "ECPRequestIDPListFinderImpl",
                "title" : "Request IDP List Finder Implementation",
                "description" : "Implementation class of the IDP list finder SPI. This returns a
list of preferred IDPs trusted by the ECP",
                "type" : "string",
                "default" : "com.sun.identity.saml2.plugins.ECPIDPFinder"
              },
              "ecpRequestIdpListGetComplete" : {
                "attributeKey" : "ECPRequestIDPListGetComplete",
                "title" : "Request IDP List Get Complete",
                "description" : "Specify an URI reference that can be used to retrieve the complete
IDP list if the IDPList element is not complete",
                "type" : "string"
              },
              "ecpRequestIdpList" : {
                "attributeKey" : "ECPRequestIDPList",
                "title" : "Request IDP List",
                "description" : "Defines a list of IDPs for the ECP to contact. This is used by the
default implementation of the IDP Finder",
                "type" : "array",
                "items" : {
                  "type" : "string"
                }
              }
            }
          },
          "idpProxy" : {
            "traverseObject" : true,
            "title" : "IDP Proxy",
            "type" : "object",
            "properties" : {
              "enableIdpProxy" : {
                "attributeKey" : "enableIDPProxy",
                "title" : "IDP Proxy enabled",
                "description" : "Enable IDP Proxy if not enabled",
                "type" : "boolean",
                "default" : false
              },
              "useIntroductionForIdpProxy" : {
                "attributeKey" : "useIntroductionForIDPProxy",
                "title" : "Introduction enabled",
                "type" : "boolean",
                "default" : false
              },
              "idpProxyCount" : {
                "attributeKey" : "idpProxyCount",
                "title" : "Proxy Count",
                "description" : "Number of IDP proxies that the SP can have",
                "type" : "integer",
```

```
                  "default" : 0
                },
                "idpProxyList" : {
                  "attributeKey" : "idpProxyList",
                  "description" : "A list of preferred IDPs that the SP would proxy to",
                  "title" : "IDP Proxy List",
                  "type" : "array",
                  "items" : {
                    "type" : "string"
                  }
                }
              }
            },
            "spSessionSyncEnabled" : {
              "attributeKey" : "spSessionSyncEnabled",
              "title" : "Session Synchronization",
              "description" : "If this is enabled, when a session times out, the Service Provider
 notifies all Identity Providers to log out. A session may time out, for example, when max-idle time
 or max-session time is reached.",
              "type" : "boolean",
              "default" : false
            },
            "relayStateUrlList" : {
              "traverseObject" : true,
              "title" : "Relay State URL List",
              "type" : "object",
              "properties" : {
                "relayStateUrlList" : {
                  "attributeKey" : "relayStateUrlList",
                  "title" : "Relay State URL List",
                  "type" : "array",
                  "items" : {
                    "type" : "string"
                  }
                }
              }
            }
          }
        }
      }
    }
  },
  "required" : [ "entityId" ],
  "$id" : "https://www.forgerock.com/hostedSaml2EntityProvider.schema.json"
}
```

HotpModule

Realm Operations

Resource path: `/realm-config/authentication/modules/hotp`

Resource version: `1.0`

create

Usage:

```
am> create HotpModule --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "otpLength" : {
      "title" : "One Time Password Length ",
      "description" : "The length of the generated One Time Password (in digits)",
      "propertyOrder" : 1000,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "otpMaxRetry" : {
      "title" : "One Time Password Max Retry",
      "description" : "The number of times entry of the OTP may be attempted. Minimum is 1 maximum is
 10 and default is 3.",
      "propertyOrder" : null,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "autoSendOTP" : {
      "title" : "Auto Send OTP Code",
      "description" : "Select this checkbox if the OTP should be sent automatically",
      "propertyOrder" : 1500,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "smtpHostname" : {
      "title" : "Mail Server Host Name",
      "description" : "The name of the mail server; OpenAM will use SMTP to send the messages.",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "userProfileEmailAttribute" : {
      "title" : "Email Attribute Name",
      "description" : "This is the attribute name used by the OTP to email the user",
      "propertyOrder" : 1400,
      "required" : true,
      "type" : "string",
```

```
      "exampleValue" : ""
    },
    "smsGatewayClass" : {
      "title" : "SMS Gateway Implementation Class",
      "description" : "The HOTP authentication module uses this class to send SMS
 messages.<br><br>The SMS gateway class must implement the following interface<br/><br/
><code>com.sun.identity.authentication.modules.hotp.SMSGateway</code>",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "smtpFromAddress" : {
      "title" : "Email From Address",
      "description" : "Emails from the HOTP Authentication module will come from this address.",
      "propertyOrder" : 800,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "otpDeliveryMethod" : {
      "title" : "One Time Password Delivery",
      "description" : "The mechanism used to deliver the One Time Password",
      "propertyOrder" : 1100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "otpValidityDuration" : {
      "title" : "One Time Password Validity Length",
      "description" : "This One Time Password will remain valid for this period (in minutes)",
      "propertyOrder" : 900,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "smtpUsername" : {
      "title" : "Mail Server Authentication Username",
      "description" : "The username to use if the mail server is using SMTP authentication",
      "propertyOrder" : 500,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "userProfileTelephoneAttribute" : {
      "title" : "Mobile Phone Number Attribute Name",
      "description" : "This is the attribute name used for a requested text message",
      "propertyOrder" : 1200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "authenticationLevel" : {
      "title" : "Authentication Level",
      "description" : "The authentication level associated with this module.<br><br>Each
 authentication module has an authentication level that can be used to indicate the level of security
 associated with the module; 0 is the lowest (and the default).",
      "propertyOrder" : 100,
      "required" : true,
```

```
      "type" : "integer",
      "exampleValue" : ""
    },
    "smtpHostPort" : {
      "title" : "Mail Server Host Port",
      "description" : "The port of the mail server.<br><br>The default port for SMTP is 25, if using
 SSL the default port is 465.",
      "propertyOrder" : 400,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "smtpSslEnabled" : {
      "title" : "Mail Server Secure Connection ",
      "description" : "This setting controls whether the authentication module communicates with the
 mail server using SSL/TLS",
      "propertyOrder" : 700,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "mobileCarrierAttribute" : {
      "title" : "Mobile Carrier Attribute Name",
      "description" : "This is the attribute name used for a mobile carrier domain for sending SMS
 messages",
      "propertyOrder" : 1300,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "smtpUserPassword" : {
      "title" : "Mail Server Authentication Password",
      "description" : "The password to use if the mail server is using SMTP authentication",
      "propertyOrder" : 600,
      "required" : true,
      "type" : "string",
      "format" : "password",
      "exampleValue" : ""
    }
  }
}
```

delete

Usage:

```
am> delete HotpModule --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action HotpModule --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action HotpModule --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action HotpModule --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query HotpModule --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read HotpModule --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update HotpModule --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "otpLength" : {
      "title" : "One Time Password Length ",
      "description" : "The length of the generated One Time Password (in digits)",
      "propertyOrder" : 1000,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "otpMaxRetry" : {
      "title" : "One Time Password Max Retry",
      "description" : "The number of times entry of the OTP may be attempted. Minimum is 1 maximum is
 10 and default is 3.",
      "propertyOrder" : null,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "autoSendOTP" : {
      "title" : "Auto Send OTP Code",
      "description" : "Select this checkbox if the OTP should be sent automatically",
      "propertyOrder" : 1500,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "smtpHostname" : {
      "title" : "Mail Server Host Name",
      "description" : "The name of the mail server; OpenAM will use SMTP to send the messages.",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "userProfileEmailAttribute" : {
      "title" : "Email Attribute Name",
      "description" : "This is the attribute name used by the OTP to email the user",
      "propertyOrder" : 1400,
      "required" : true,
      "type" : "string",
```

```
      "exampleValue" : ""
    },
    "smsGatewayClass" : {
      "title" : "SMS Gateway Implementation Class",
      "description" : "The HOTP authentication module uses this class to send SMS
 messages.<br><br>The SMS gateway class must implement the following interface<br/><br/
><code>com.sun.identity.authentication.modules.hotp.SMSGateway</code>",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "smtpFromAddress" : {
      "title" : "Email From Address",
      "description" : "Emails from the HOTP Authentication module will come from this address.",
      "propertyOrder" : 800,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "otpDeliveryMethod" : {
      "title" : "One Time Password Delivery",
      "description" : "The mechanism used to deliver the One Time Password",
      "propertyOrder" : 1100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "otpValidityDuration" : {
      "title" : "One Time Password Validity Length",
      "description" : "This One Time Password will remain valid for this period (in minutes)",
      "propertyOrder" : 900,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "smtpUsername" : {
      "title" : "Mail Server Authentication Username",
      "description" : "The username to use if the mail server is using SMTP authentication",
      "propertyOrder" : 500,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "userProfileTelephoneAttribute" : {
      "title" : "Mobile Phone Number Attribute Name",
      "description" : "This is the attribute name used for a requested text message",
      "propertyOrder" : 1200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "authenticationLevel" : {
      "title" : "Authentication Level",
      "description" : "The authentication level associated with this module.<br><br>Each
 authentication module has an authentication level that can be used to indicate the level of security
 associated with the module; 0 is the lowest (and the default).",
      "propertyOrder" : 100,
      "required" : true,
```

```
      "type" : "integer",
      "exampleValue" : ""
    },
    "smtpHostPort" : {
      "title" : "Mail Server Host Port",
      "description" : "The port of the mail server.<br><br>The default port for SMTP is 25, if using
 SSL the default port is 465.",
      "propertyOrder" : 400,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "smtpSslEnabled" : {
      "title" : "Mail Server Secure Connection ",
      "description" : "This setting controls whether the authentication module communicates with the
 mail server using SSL/TLS",
      "propertyOrder" : 700,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "mobileCarrierAttribute" : {
      "title" : "Mobile Carrier Attribute Name",
      "description" : "This is the attribute name used for a mobile carrier domain for sending SMS
 messages",
      "propertyOrder" : 1300,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "smtpUserPassword" : {
      "title" : "Mail Server Authentication Password",
      "description" : "The password to use if the mail server is using SMTP authentication",
      "propertyOrder" : 600,
      "required" : true,
      "type" : "string",
      "format" : "password",
      "exampleValue" : ""
    }
  }
}
```

Global Operations

Resource path: `/global-config/authentication/modules/hotp`

Resource version: `1.0`

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action HotpModule --global --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action HotpModule --global --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action HotpModule --global --actionName nextdescendents
```

read

Usage:

```
am> read HotpModule --global
```

update

Usage:

```
am> update HotpModule --global --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "defaults" : {
      "properties" : {
        "smtpUserPassword" : {
          "title" : "Mail Server Authentication Password",
          "description" : "The password to use if the mail server is using SMTP authentication",
          "propertyOrder" : 600,
          "required" : true,
          "type" : "string",
          "format" : "password",
          "exampleValue" : ""
        },
        "otpValidityDuration" : {
```

```
          "title" : "One Time Password Validity Length",
          "description" : "This One Time Password will remain valid for this period (in minutes)",
          "propertyOrder" : 900,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "smsGatewayClass" : {
          "title" : "SMS Gateway Implementation Class",
          "description" : "The HOTP authentication module uses this class to send SMS
 messages.<br><br>The SMS gateway class must implement the following interface<br/><br/
><code>com.sun.identity.authentication.modules.hotp.SMSGateway</code>",
          "propertyOrder" : 200,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "smtpFromAddress" : {
          "title" : "Email From Address",
          "description" : "Emails from the HOTP Authentication module will come from this address.",
          "propertyOrder" : 800,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "smtpUsername" : {
          "title" : "Mail Server Authentication Username",
          "description" : "The username to use if the mail server is using SMTP authentication",
          "propertyOrder" : 500,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "otpLength" : {
          "title" : "One Time Password Length ",
          "description" : "The length of the generated One Time Password (in digits)",
          "propertyOrder" : 1000,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "userProfileEmailAttribute" : {
          "title" : "Email Attribute Name",
          "description" : "This is the attribute name used by the OTP to email the user",
          "propertyOrder" : 1400,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "otpMaxRetry" : {
          "title" : "One Time Password Max Retry",
          "description" : "The number of times entry of the OTP may be attempted. Minimum is 1 maximum
 is 10 and default is 3.",
          "propertyOrder" : null,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "autoSendOTP" : {
```

```
          "title" : "Auto Send OTP Code",
          "description" : "Select this checkbox if the OTP should be sent automatically",
          "propertyOrder" : 1500,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "authenticationLevel" : {
          "title" : "Authentication Level",
          "description" : "The authentication level associated with this module.<br><br>Each
authentication module has an authentication level that can be used to indicate the level of security
associated with the module; 0 is the lowest (and the default).",
          "propertyOrder" : 100,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "smtpHostPort" : {
          "title" : "Mail Server Host Port",
          "description" : "The port of the mail server.<br><br>The default port for SMTP is 25, if
using SSL the default port is 465.",
          "propertyOrder" : 400,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "smtpSslEnabled" : {
          "title" : "Mail Server Secure Connection ",
          "description" : "This setting controls whether the authentication module communicates with
the mail server using SSL/TLS",
          "propertyOrder" : 700,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "mobileCarrierAttribute" : {
          "title" : "Mobile Carrier Attribute Name",
          "description" : "This is the attribute name used for a mobile carrier domain for sending SMS
messages",
          "propertyOrder" : 1300,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "smtpHostname" : {
          "title" : "Mail Server Host Name",
          "description" : "The name of the mail server; OpenAM will use SMTP to send the messages.",
          "propertyOrder" : 300,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "otpDeliveryMethod" : {
          "title" : "One Time Password Delivery",
          "description" : "The mechanism used to deliver the One Time Password",
          "propertyOrder" : 1100,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
```

```
        },
        "userProfileTelephoneAttribute" : {
          "title" : "Mobile Phone Number Attribute Name",
          "description" : "This is the attribute name used for a requested text message",
          "propertyOrder" : 1200,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      },
      "type" : "object",
      "title" : "Realm Defaults"
    }
  }
}
```

HsmMappings

Realm Operations

Resource path: `/realm-config/secrets/stores/HsmSecretStore/{HsmSecretStore}/mappings`

Resource version: `1.0`

create

Usage:

```
am> create HsmMappings --realm Realm --HsmSecretStore HsmSecretStore --id id --body body
```

Parameters:

--HsmSecretStore

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "aliases" : {
      "title" : "Aliases",
      "description" : "The list of keystore aliases that can resolve the secret. The first element of
 the alias list determines which alias is the \"active\" one. Active secrets are used for signature
 generation and encryption, while the non-active secrets are mainly used for signature verification
 and decryption.",
      "propertyOrder" : 200,
      "required" : true,
      "items" : {
        "type" : "string",
        "minLength" : 1
      },
      "minItems" : 1,
      "uniqueItems" : true,
      "type" : "array",
      "exampleValue" : ""
    },
    "secretId" : {
      "title" : "Secret ID",
      "description" : "The secret ID that is to be associated with an alias.",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
```

delete

Usage:

```
am> delete HsmMappings --realm Realm --HsmSecretStore HsmSecretStore --id id
```

Parameters:

--HsmSecretStore

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action HsmMappings --realm Realm --HsmSecretStore HsmSecretStore --actionName getAllTypes
```

Parameters:

--HsmSecretStore

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action HsmMappings --realm Realm --HsmSecretStore HsmSecretStore --actionName getCreatableTypes
```

Parameters:

--HsmSecretStore

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action HsmMappings --realm Realm --HsmSecretStore HsmSecretStore --actionName nextdescendents
```

Parameters:

--HsmSecretStore

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query HsmMappings --realm Realm --filter filter --HsmSecretStore HsmSecretStore
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

--HsmSecretStore

read

Usage:

```
am> read HsmMappings --realm Realm --HsmSecretStore HsmSecretStore --id id
```

Parameters:

--HsmSecretStore

--id

The unique identifier for the resource.

update

Usage:

```
am> update HsmMappings --realm Realm --HsmSecretStore HsmSecretStore --id id --body body
```

Parameters:

--HsmSecretStore

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "aliases" : {
      "title" : "Aliases",
      "description" : "The list of keystore aliases that can resolve the secret. The first element of
 the alias list determines which alias is the \"active\" one. Active secrets are used for signature
 generation and encryption, while the non-active secrets are mainly used for signature verification
 and decryption.",
      "propertyOrder" : 200,
      "required" : true,
      "items" : {
        "type" : "string",
        "minLength" : 1
      },
      "minItems" : 1,
      "uniqueItems" : true,
      "type" : "array",
      "exampleValue" : ""
    },
    "secretId" : {
      "title" : "Secret ID",
      "description" : "The secret ID that is to be associated with an alias.",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
```


Global Operations

Resource path: `/global-config/secrets/stores/HsmSecretStore/{HsmSecretStore}/mappings`

Resource version: `1.0`

create

Usage:

```
am> create HsmMappings --global --HsmSecretStore HsmSecretStore --id id --body body
```

Parameters:

--HsmSecretStore

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "secretId" : {
      "title" : "Secret ID",
      "description" : "The secret ID that is to be associated with an alias.",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "aliases" : {
      "title" : "Aliases",
      "description" : "The list of keystore aliases that can resolve the secret. The first element of
 the alias list determines which alias is the \"active\" one. Active secrets are used for signature
 generation and encryption, while the non-active secrets are mainly used for signature verification
 and decryption.",
      "propertyOrder" : 200,
      "required" : true,
      "items" : {
        "type" : "string",
        "minLength" : 1
      },
      "minItems" : 1,
      "uniqueItems" : true,
      "type" : "array",
      "exampleValue" : ""
    }
  }
}
```

delete

Usage:

```
am> delete HsmMappings --global --HsmSecretStore HsmSecretStore --id id
```

Parameters:

--HsmSecretStore

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action HsmMappings --global --HsmSecretStore HsmSecretStore --actionName getAllTypes
```

Parameters:

--HsmSecretStore

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action HsmMappings --global --HsmSecretStore HsmSecretStore --actionName getCreatableTypes
```

Parameters:

--HsmSecretStore

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action HsmMappings --global --HsmSecretStore HsmSecretStore --actionName nextdescendents
```

Parameters:

--HsmSecretStore

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query HsmMappings --global --filter filter --HsmSecretStore HsmSecretStore
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

--HsmSecretStore

read

Usage:

```
am> read HsmMappings --global --HsmSecretStore HsmSecretStore --id id
```

Parameters:

--HsmSecretStore

--id

The unique identifier for the resource.

update

Usage:

```
am> update HsmMappings --global --HsmSecretStore HsmSecretStore --id id --body body
```

Parameters:

--HsmSecretStore

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "secretId" : {
      "title" : "Secret ID",
      "description" : "The secret ID that is to be associated with an alias.",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "aliases" : {
      "title" : "Aliases",
      "description" : "The list of keystore aliases that can resolve the secret. The first element of
 the alias list determines which alias is the \"active\" one. Active secrets are used for signature
 generation and encryption, while the non-active secrets are mainly used for signature verification
 and decryption.",
      "propertyOrder" : 200,
      "required" : true,
      "items" : {
        "type" : "string",
        "minLength" : 1
      },
      "minItems" : 1,
      "uniqueItems" : true,
      "type" : "array",
      "exampleValue" : ""
    }
  }
}
```

HsmSecretStore

Realm Operations

Resource path: `/realm-config/secrets/stores/HsmSecretStore`

Resource version: `1.0`

create

Usage:

```
am> create HsmSecretStore --realm Realm --id id --body body
```

Parameters:

`--id`

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "storePassword" : {
      "title" : "HSM PIN/password secret ID",
      "description" : "The secret ID using which the HSM's PIN/password can be obtained. This secret
 ID will be resolved using one of the other secret stores configured.<br> It must not start or end
 with the <code>.</code> character. <br>The <code>.</code> character must not be followed by another
 <code>.</code> character.<br>Must contain <code>a-z</code>, <code>A-Z</code>, <code>0-9</code> and
 <code>.</code> characters only.",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "providerGuiceKey" : {
      "title" : "Provider Guice Key Name",
      "description" : "The name of a Guice key that can be used to obtain an initialised provider from
 which the HSM keystore can be obtained.",
      "propertyOrder" : 200,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
    },
    "leaseExpiryDuration" : {
      "title" : "Key lease expiry",
      "description" : "The amount of minutes a key can be cached from the keystore before it needs to
 be reloaded.",
      "propertyOrder" : 400,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "file" : {
      "title" : "Configuration File",
      "description" : "The file containing initialisation configuration for the HSM.",
      "propertyOrder" : 100,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
```

delete

Usage:

```
am> delete HsmSecretStore --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action HsmSecretStore --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action HsmSecretStore --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action HsmSecretStore --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query HsmSecretStore --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read HsmSecretStore --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update HsmSecretStore --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "storePassword" : {
      "title" : "HSM PIN/password secret ID",
      "description" : "The secret ID using which the HSM's PIN/password can be obtained. This secret
 ID will be resolved using one of the other secret stores configured.<br> It must not start or end
 with the <code>.</code> character. <br>The <code>.</code> character must not be followed by another
 <code>.</code> character.<br>Must contain <code>a-z</code>, <code>A-Z</code>, <code>0-9</code> and
 <code>.</code> characters only.",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "providerGuiceKey" : {
      "title" : "Provider Guice Key Name",
      "description" : "The name of a Guice key that can be used to obtain an initialised provider from
 which the HSM keystore can be obtained.",
      "propertyOrder" : 200,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
    },
    "leaseExpiryDuration" : {
      "title" : "Key lease expiry",
      "description" : "The amount of minutes a key can be cached from the keystore before it needs to
 be reloaded.",
      "propertyOrder" : 400,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
```

```
    },
    "file" : {
      "title" : "Configuration File",
      "description" : "The file containing initialisation configuration for the HSM.",
      "propertyOrder" : 100,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
```

Global Operations

Resource path: `/global-config/secrets/stores/HsmSecretStore`

Resource version: `1.0`

create

Usage:

```
am> create HsmSecretStore --global --id id --body body
```

Parameters:

`--id`

The unique identifier for the resource.

`--body`

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "leaseExpiryDuration" : {
      "title" : "Key lease expiry",
      "description" : "The amount of minutes a key can be cached from the keystore before it needs to
 be reloaded.",
      "propertyOrder" : 400,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "file" : {
      "title" : "Configuration File",
      "description" : "The file containing initialisation configuration for the HSM.",
      "propertyOrder" : 100,
      "required" : false,
      "type" : "string",
```

```
      "exampleValue" : ""
    },
    "providerGuiceKey" : {
      "title" : "Provider Guice Key Name",
      "description" : "The name of a Guice key that can be used to obtain an initialised provider from
 which the HSM keystore can be obtained.",
      "propertyOrder" : 200,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
    },
    "storePassword" : {
      "title" : "HSM PIN/password secret ID",
      "description" : "The secret ID using which the HSM's PIN/password can be obtained. This secret
 ID will be resolved using one of the other secret stores configured.<br> It must not start or end
 with the <code>.</code> character. <br>The <code>.</code> character must not be followed by another
 <code>.</code> character.<br>Must contain <code>a-z</code>, <code>A-Z</code>, <code>0-9</code> and
 <code>.</code> characters only.",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
```


delete

Usage:

```
am> delete HsmSecretStore --global --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action HsmSecretStore --global --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action HsmSecretStore --global --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action HsmSecretStore --global --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query HsmSecretStore --global --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read HsmSecretStore --global --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update HsmSecretStore --global --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "leaseExpiryDuration" : {
      "title" : "Key lease expiry",
      "description" : "The amount of minutes a key can be cached from the keystore before it needs to
 be reloaded.",
      "propertyOrder" : 400,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "file" : {
      "title" : "Configuration File",
      "description" : "The file containing initialisation configuration for the HSM.",
      "propertyOrder" : 100,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
    },
    "providerGuiceKey" : {
      "title" : "Provider Guice Key Name",
      "description" : "The name of a Guice key that can be used to obtain an initialised provider from
 which the HSM keystore can be obtained.",
      "propertyOrder" : 200,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
    },
    "storePassword" : {
      "title" : "HSM PIN/password secret ID",
      "description" : "The secret ID using which the HSM's PIN/password can be obtained. This secret
 ID will be resolved using one of the other secret stores configured.<br> It must not start or end
 with the <code>.</code> character. <br>The <code>.</code> character must not be followed by another
 <code>.</code> character.<br>Must contain <code>a-z</code>, <code>A-Z</code>, <code>0-9</code> and
 <code>.</code> characters only.",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
```

HttpBasicModule

Realm Operations

Resource path: `/realm-config/authentication/modules/httpbasic`

Resource version: `1.0`

create

Usage:

```
am> create HttpBasicModule --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "backendModuleName" : {
      "title" : "Backend Module Name",
      "description" : "The name of the module that will be used to perform the
 authentication<br><br>The HTTP Basic authentication module collect the credentials from the user and
 will then supply said credentials to the backend authentication module using the shared state. ",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "authenticationLevel" : {
      "title" : "Authentication Level",
      "description" : "The authentication level associated with this module.<br><br>Each
 authentication module has an authentication level that can be used to indicate the level of security
 associated with the module; 0 is the lowest (and the default). ",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    }
  }
}
```

delete

Usage:

```
am> delete HttpBasicModule --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action HttpBasicModule --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action HttpBasicModule --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action HttpBasicModule --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query HttpBasicModule --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read HttpBasicModule --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update HttpBasicModule --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "backendModuleName" : {
      "title" : "Backend Module Name",
      "description" : "The name of the module that will be used to perform the
 authentication<br><br>The HTTP Basic authentication module collect the credentials from the user and
 will then supply said credentials to the backend authentication module using the shared state. ",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "authenticationLevel" : {
      "title" : "Authentication Level",
      "description" : "The authentication level associated with this module.<br><br>Each
 authentication module has an authentication level that can be used to indicate the level of security
 associated with the module; 0 is the lowest (and the default). ",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    }
  }
}
```

Global Operations

Resource path: `/global-config/authentication/modules/httpbasic`

Resource version: `1.0`

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action HttpBasicModule --global --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action HttpBasicModule --global --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action HttpBasicModule --global --actionName nextdescendents
```

read

Usage:

```
am> read HttpBasicModule --global
```

update

Usage:

```
am> update HttpBasicModule --global --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "defaults" : {
      "properties" : {
        "backendModuleName" : {
          "title" : "Backend Module Name",
          "description" : "The name of the module that will be used to perform the
 authentication<br><br>The HTTP Basic authentication module collect the credentials from the user and
 will then supply said credentials to the backend authentication module using the shared state. ",
          "propertyOrder" : 100,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "authenticationLevel" : {
          "title" : "Authentication Level",
          "description" : "The authentication level associated with this module.<br><br>Each
 authentication module has an authentication level that can be used to indicate the level of security
 associated with the module; 0 is the lowest (and the default). ",
          "propertyOrder" : 200,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        }
      },
      "type" : "object",
      "title" : "Realm Defaults"
    }
  }
}
```

IDMProvisioning

Global Operations

Resource path: `/global-config/services/idm-integration`

Resource version: `1.0`

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action IDMProvisioning --global --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action IDMProvisioning --global --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action IDMProvisioning --global --actionName nextdescendents
```

read

Usage:

```
am> read IDMProvisioning --global
```

update

Usage:

```
am> update IDMProvisioning --global --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "provisioningSigningKeyAlias" : {
      "title" : "Signing Key Alias",
      "description" : "Alias of the signing symmetric key in AM's default keystore. Must be a
 duplicate of the symmetric key used by IDM.",
      "propertyOrder" : 500,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "idmDeploymentPath" : {
      "title" : "Deployment Path",
      "description" : "Path of the IDM deployment, e.g. openidm",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
```

```
    },
    "enabled" : {
      "title" : "Enabled",
      "description" : "",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "provisioningEncryptionAlgorithm" : {
      "title" : "Encryption Algorithm",
      "description" : "JWT encryption algorithm.",
      "propertyOrder" : 900,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "provisioningEncryptionKeyAlias" : {
      "title" : "Encryption Key Alias",
      "description" : "Alias of the encryption asymmetric key in AM's default keystore. Must be a
duplicate of the asymmetric key used by IDM.",
      "propertyOrder" : 600,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "provisioningSigningAlgorithm" : {
      "title" : "Signing Algorithm",
      "description" : "JWT signing algorithm.",
      "propertyOrder" : 700,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "jwtSigningCompatibilityMode" : {
      "title" : "Signing Compatibility Mode",
      "description" : "Enable OpenAM to communicate with OpenIDM 6 and earlier.<br><br>When this
option is enabled, OpenAM will sign JWTs in a way that is compatible with versions of OpenIDM 6 and
earlier.  The approach used is incompatible with non-extractable HSM keys.  Disable this option if
you have upgraded to OpenIDM 6.5, or later.",
      "propertyOrder" : 800,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "idmDeploymentUrl" : {
      "title" : "Deployment URL",
      "description" : "URL of the IDM deployment, e.g. https://localhost:8080",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "idmProvisioningClient" : {
      "title" : "IDM Provisioning Client",
      "description" : "The name of the oauth client to be used for the client credentials flow",
      "propertyOrder" : 400,
      "required" : true,
      "type" : "string",
```

```
      "exampleValue" : ""
    },
    "provisioningEncryptionMethod" : {
      "title" : "Encryption Method",
      "description" : "JWT encryption method.",
      "propertyOrder" : 1000,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
```

IdRepository

Realm Operations

Resource path: `/realm-config/services/id-repositories`

Resource version: `1.0`

create

Usage:

```
am> create IdRepository --realm Realm --body body
```

Parameters:

`--body`

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "sunIdRepoAttributeValidator" : {
      "title" : "Attribute Validator Plug-in",
      "description" : "",
      "propertyOrder" : 300,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "sunIdRepoAttributeCombiner" : {
      "title" : "Attribute Combiner plug-in",
      "description" : "",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
```

delete

Usage:

```
am> delete IdRepository --realm Realm
```

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action IdRepository --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action IdRepository --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action IdRepository --realm Realm --actionName nextdescendents
```

read

Usage:

```
am> read IdRepository --realm Realm
```

update

Usage:

```
am> update IdRepository --realm Realm --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "sunIdRepoAttributeValidator" : {
      "title" : "Attribute Validator Plug-in",
      "description" : "",
      "propertyOrder" : 300,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "sunIdRepoAttributeCombiner" : {
      "title" : "Attribute Combiner plug-in",
      "description" : "",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
```

Global Operations

Resource path: `/global-config/services/id-repositories`

Resource version: `1.0`

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action IdRepository --global --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action IdRepository --global --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action IdRepository --global --actionName nextdescendents
```

read

Usage:

```
am> read IdRepository --global
```

update

Usage:

```
am> update IdRepository --global --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "defaults" : {
      "properties" : {
        "sunIdRepoAttributeCombiner" : {
          "title" : "Attribute Combiner plug-in",
          "description" : "",
          "propertyOrder" : 100,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "sunIdRepoAttributeValidator" : {
          "title" : "Attribute Validator Plug-in",
          "description" : "",
          "propertyOrder" : 300,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        }
      },
      "type" : "object",
      "title" : "Realm Defaults"
    }
  }
}
```

IdRepositoryUser

Global Operations

Resource path: `/global-config/services/id-repositories/user`

Resource version: `1.0`

create

Usage:

```
am> create IdRepositoryUser --global --id id --body body
```

Parameters:

`--id`

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "userPassword" : {
      "title" : "Password",
      "description" : "",
      "propertyOrder" : 9400,
      "required" : true,
      "type" : "string",
      "format" : "password",
      "exampleValue" : ""
    },
    "telephoneNumber" : {
      "title" : "Telephone Number",
      "description" : "",
      "propertyOrder" : 9700,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
    },
    "iplanet-am-user-success-url" : {
      "title" : "Success URL",
      "description" : "URL or ClientType|URL if client specific. URL without http(s) protocol will be
 appended to the current URI.",
      "propertyOrder" : 10200,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
    },
    "sn" : {
      "title" : "Last Name",
      "description" : "",
      "propertyOrder" : 9100,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
    },
    "lastEmailSent" : {
      "title" : "lastEmailSent",
      "description" : "",
      "propertyOrder" : 9800,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
    },
    "sunIdentityMSISDNNumber" : {
      "title" : "MSISDN Number",
      "description" : "",
      "propertyOrder" : 10400,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
    },
    "mail" : {
      "title" : "Email Address",
```

```
      "description" : "",
      "propertyOrder" : 9500,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
    },
    "givenName" : {
      "title" : "First Name",
      "description" : "",
      "propertyOrder" : 9000,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
    },
    "inetUserStatus" : {
      "title" : "User Status",
      "description" : "",
      "propertyOrder" : 9900,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "dn" : {
      "title" : "DN",
      "description" : "",
      "propertyOrder" : 9300,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
    },
    "postalAddress" : {
      "title" : "Home Address",
      "description" : "",
      "propertyOrder" : 9800,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
    },
    "retryLimitNodeCount" : {
      "title" : "retryLimitNodeCount",
      "description" : "",
      "propertyOrder" : 9900,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
    },
    "employeeNumber" : {
      "title" : "Employee Number",
      "description" : "",
      "propertyOrder" : 9600,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
    },
    "roles" : {
      "title" : "Roles",
      "description" : "",
      "propertyOrder" : 10500,
      "required" : false,
```

```
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "iplanet-am-user-failure-url" : {
      "title" : "Failure URL",
      "description" : "URL or ClientType|URL if client specific. URL without http(s) protocol will be
 appended to the current URI.",
      "propertyOrder" : 10300,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
    },
    "iplanet-am-user-alias-list" : {
      "title" : "User Alias List",
      "description" : "",
      "propertyOrder" : 10100,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
    },
    "iplanet-am-user-auth-config" : {
      "title" : "Authentication Configuration",
      "description" : "",
      "propertyOrder" : 10000,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "cn" : {
      "title" : "Full Name",
      "description" : "",
      "propertyOrder" : 9200,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
```


delete

Usage:

```
am> delete IdRepositoryUser --global --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action IdRepositoryUser --global --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action IdRepositoryUser --global --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action IdRepositoryUser --global --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query IdRepositoryUser --global --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read IdRepositoryUser --global --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update IdRepositoryUser --global --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "userPassword" : {
      "title" : "Password",
      "description" : "",
      "propertyOrder" : 9400,
      "required" : true,
      "type" : "string",
      "format" : "password",
      "exampleValue" : ""
    },
    "telephoneNumber" : {
      "title" : "Telephone Number",
      "description" : "",
      "propertyOrder" : 9700,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
    },
    "iplanet-am-user-success-url" : {
      "title" : "Success URL",
      "description" : "URL or ClientType|URL if client specific. URL without http(s) protocol will be
 appended to the current URI.",
      "propertyOrder" : 10200,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
    },
    "sn" : {
      "title" : "Last Name",
      "description" : "",
      "propertyOrder" : 9100,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
    },
    "lastEmailSent" : {
      "title" : "lastEmailSent",
      "description" : "",
      "propertyOrder" : 9800,
      "required" : false,
```

```
      "type" : "string",
      "exampleValue" : ""
    },
    "sunIdentityMSISDNNumber" : {
      "title" : "MSISDN Number",
      "description" : "",
      "propertyOrder" : 10400,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
    },
    "mail" : {
      "title" : "Email Address",
      "description" : "",
      "propertyOrder" : 9500,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
    },
    "givenName" : {
      "title" : "First Name",
      "description" : "",
      "propertyOrder" : 9000,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
    },
    "inetUserStatus" : {
      "title" : "User Status",
      "description" : "",
      "propertyOrder" : 9900,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "dn" : {
      "title" : "DN",
      "description" : "",
      "propertyOrder" : 9300,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
    },
    "postalAddress" : {
      "title" : "Home Address",
      "description" : "",
      "propertyOrder" : 9800,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
    },
    "retryLimitNodeCount" : {
      "title" : "retryLimitNodeCount",
      "description" : "",
      "propertyOrder" : 9900,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
    },
```

```
    "employeeNumber" : {
      "title" : "Employee Number",
      "description" : "",
      "propertyOrder" : 9600,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
    },
    "roles" : {
      "title" : "Roles",
      "description" : "",
      "propertyOrder" : 10500,
      "required" : false,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "iplanet-am-user-failure-url" : {
      "title" : "Failure URL",
      "description" : "URL or ClientType|URL if client specific. URL without http(s) protocol will be
 appended to the current URI.",
      "propertyOrder" : 10300,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
    },
    "iplanet-am-user-alias-list" : {
      "title" : "User Alias List",
      "description" : "",
      "propertyOrder" : 10100,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
    },
    "iplanet-am-user-auth-config" : {
      "title" : "Authentication Configuration",
      "description" : "",
      "propertyOrder" : 10000,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "cn" : {
      "title" : "Full Name",
      "description" : "",
      "propertyOrder" : 9200,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
```

IdentifyExistingUser

Realm Operations

Resource path: `/realm-config/authentication/authenticationtrees/nodes/IdentifyExistingUserNode`

Resource version: `1.0`

create

Usage:

```
am> create IdentifyExistingUser --realm Realm --id id --body body
```

Parameters:

`--id`

The unique identifier for the resource.

`--body`

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "identifier" : {
      "title" : "Identifier",
      "description" : "The IDM attribute used to save existing value in sharedState for log in
 purposes.",
      "propertyOrder" : 100,
      "type" : "string",
      "exampleValue" : ""
    },
    "identityAttribute" : {
      "title" : "Identity Attribute",
      "description" : "The attribute used to retrieve an existing user.",
      "propertyOrder" : 200,
      "type" : "string",
      "exampleValue" : ""
    }
  },
  "required" : [ "identifier", "identityAttribute" ]
}
```

delete

Usage:

```
am> delete IdentifyExistingUser --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action IdentifyExistingUser --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action IdentifyExistingUser --realm Realm --actionName getCreatableTypes
```

listOutcomes

List the available outcomes for the node type.

Usage:

```
am> action IdentifyExistingUser --realm Realm --body body --actionName listOutcomes
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "title" : "Some configuration of the node. This does not need to be complete against the
 configuration schema."
}
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action IdentifyExistingUser --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query IdentifyExistingUser --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read IdentifyExistingUser --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update IdentifyExistingUser --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "identifier" : {
      "title" : "Identifier",
      "description" : "The IDM attribute used to save existing value in sharedState for log in
 purposes.",
      "propertyOrder" : 100,
      "type" : "string",
      "exampleValue" : ""
    },
    "identityAttribute" : {
      "title" : "Identity Attribute",
      "description" : "The attribute used to retrieve an existing user.",
      "propertyOrder" : 200,
      "type" : "string",
      "exampleValue" : ""
    }
  },
  "required" : [ "identifier", "identityAttribute" ]
}
```

IdentityGatewayAgentGroups

Realm Operations

Agent Groups handler that is responsible for managing agent groups

Resource path: `/realm-config/agents/groups/IdentityGatewayAgent`

Resource version: `1.0`

create

Usage:

```
am> create IdentityGatewayAgentGroups --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
```

```
  "type" : "object",
  "properties" : {
    "status" : {
      "title" : "Status",
      "description" : "Status of the agent configuration.",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "igCdssoRedirectUrls" : {
      "title" : "Redirect URLs for CDSSO",
      "description" : "The list of redirect URLs for CDSSO. The valid value is in the following
 format: <br>protocol://hostname:port/path<br> The protocol represents the protocol used, such as
 http or https. The hostname represents the host name of the machine on which IG resides. The port
 represents the port number on which IG is listening. The path represents the remainder of the
 redirect URL. <br>Example:<br> http://openig.ext.com:8080/home/cdsso/redirect",
      "propertyOrder" : 150,
      "required" : false,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "igTokenIntrospection" : {
      "title" : "Token Introspection",
      "description" : "Allows using this IG agent to introspect OAuth 2.0 tokens issued to any client.
 <br>Select <code>None</code> to disable. Select <code>Realm Only</code> to allow introspection of
 tokens in the same realm. Select <code>Realm and Sub Realms</code> to allow introspection of tokens
 in the same realm and any sub-realms.",
      "propertyOrder" : 160,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
```

delete

Usage:

```
am> delete IdentityGatewayAgentGroups --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action IdentityGatewayAgentGroups --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action IdentityGatewayAgentGroups --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action IdentityGatewayAgentGroups --realm Realm --actionName nextdescendents
```

query

Querying the agent groups of a specific type

Usage:

```
am> query IdentityGatewayAgentGroups --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read IdentityGatewayAgentGroups --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update IdentityGatewayAgentGroups --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "status" : {
      "title" : "Status",
      "description" : "Status of the agent configuration.",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "igCdssoRedirectUrls" : {
      "title" : "Redirect URLs for CDSSO",
      "description" : "The list of redirect URLs for CDSSO. The valid value is in the following
 format: <br>protocol://hostname:port/path<br> The protocol represents the protocol used, such as
 http or https. The hostname represents the host name of the machine on which IG resides. The port
 represents the port number on which IG is listening. The path represents the remainder of the
 redirect URL. <br>Example:<br> http://openig.ext.com:8080/home/cdsso/redirect",
      "propertyOrder" : 150,
      "required" : false,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "igTokenIntrospection" : {
      "title" : "Token Introspection",
      "description" : "Allows using this IG agent to introspect OAuth 2.0 tokens issued to any client.
 <br>Select <code>None</code> to disable. Select <code>Realm Only</code> to allow introspection of
 tokens in the same realm. Select <code>Realm and Sub Realms</code> to allow introspection of tokens
 in the same realm and any sub-realms.",
      "propertyOrder" : 160,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
```

IdentityGatewayAgents

Realm Operations

Agents handler that is responsible for managing agents

Resource path: `/realm-config/agents/IdentityGatewayAgent`

Resource version: `1.0`

create

Usage:

```
am> create IdentityGatewayAgents --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "status" : {
      "title" : "Status",
      "description" : "Status of the agent configuration.",
      "propertyOrder" : 200,
      "type" : "object",
      "exampleValue" : "",
      "properties" : {
        "inherited" : {
          "type" : "boolean",
          "required" : true
        },
        "value" : {
          "type" : "string",
          "required" : true
        }
      }
    },
    "igTokenIntrospection" : {
      "title" : "Token Introspection",
      "description" : "Allows using this IG agent to introspect OAuth 2.0 tokens issued to any client.
<br>Select <code>None</code> to disable. Select <code>Realm Only</code> to allow introspection of
tokens in the same realm. Select <code>Realm and Sub Realms</code> to allow introspection of tokens
in the same realm and any sub-realms.",
      "propertyOrder" : 160,
      "type" : "object",
```

```
      "exampleValue" : "",
      "properties" : {
        "inherited" : {
          "type" : "boolean",
          "required" : true
        },
        "value" : {
          "type" : "string",
          "required" : false
        }
      }
    },
    "agentgroup" : {
      "title" : "Group",
      "description" : "Add the agent to a group to allow inheritance of property values from the
 group. <br>Changing the group will update inherited property values. <br>Inherited property values
 are copied to the agent.",
      "propertyOrder" : 50,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
    },
    "igCdssoRedirectUrls" : {
      "title" : "Redirect URLs for CDSSO",
      "description" : "The list of redirect URLs for CDSSO. The valid value is in the following
 format: <br>protocol://hostname:port/path<br> The protocol represents the protocol used, such as
 http or https. The hostname represents the host name of the machine on which IG resides. The port
 represents the port number on which IG is listening. The path represents the remainder of the
 redirect URL. <br>Example:<br> http://openig.ext.com:8080/home/cdsso/redirect",
      "propertyOrder" : 150,
      "items" : {
        "type" : "string"
      },
      "type" : "object",
      "exampleValue" : "",
      "properties" : {
        "inherited" : {
          "type" : "boolean",
          "required" : true
        },
        "value" : {
          "type" : "array",
          "required" : false
        }
      }
    },
    "userpassword" : {
      "title" : "Password",
      "description" : "",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "format" : "password",
      "exampleValue" : ""
    }
  }
}
```

delete

Usage:

```
am> delete IdentityGatewayAgents --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action IdentityGatewayAgents --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action IdentityGatewayAgents --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action IdentityGatewayAgents --realm Realm --actionName nextdescendents
```

query

Querying the agents of a specific type

Usage:

```
am> query IdentityGatewayAgents --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read IdentityGatewayAgents --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update IdentityGatewayAgents --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "status" : {
      "title" : "Status",
      "description" : "Status of the agent configuration.",
      "propertyOrder" : 200,
      "type" : "object",
      "exampleValue" : "",
      "properties" : {
        "inherited" : {
          "type" : "boolean",
          "required" : true
        },
        "value" : {
          "type" : "string",
          "required" : true
        }
      }
    },
    "igTokenIntrospection" : {
      "title" : "Token Introspection",
      "description" : "Allows using this IG agent to introspect OAuth 2.0 tokens issued to any client.
<br>Select <code>None</code> to disable. Select <code>Realm Only</code> to allow introspection of
tokens in the same realm. Select <code>Realm and Sub Realms</code> to allow introspection of tokens
in the same realm and any sub-realms.",
      "propertyOrder" : 160,
```

```
      "type" : "object",
      "exampleValue" : "",
      "properties" : {
        "inherited" : {
          "type" : "boolean",
          "required" : true
        },
        "value" : {
          "type" : "string",
          "required" : false
        }
      }
    },
    "agentgroup" : {
      "title" : "Group",
      "description" : "Add the agent to a group to allow inheritance of property values from the
 group. <br>Changing the group will update inherited property values. <br>Inherited property values
 are copied to the agent.",
      "propertyOrder" : 50,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
    },
    "igCdssoRedirectUrls" : {
      "title" : "Redirect URLs for CDSSO",
      "description" : "The list of redirect URLs for CDSSO. The valid value is in the following
 format: <br>protocol://hostname:port/path<br> The protocol represents the protocol used, such as
 http or https. The hostname represents the host name of the machine on which IG resides. The port
 represents the port number on which IG is listening. The path represents the remainder of the
 redirect URL. <br>Example:<br> http://openig.ext.com:8080/home/cdsso/redirect",
      "propertyOrder" : 150,
      "items" : {
        "type" : "string"
      },
      "type" : "object",
      "exampleValue" : "",
      "properties" : {
        "inherited" : {
          "type" : "boolean",
          "required" : true
        },
        "value" : {
          "type" : "array",
          "required" : false
        }
      }
    },
    "userpassword" : {
      "title" : "Password",
      "description" : "",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "format" : "password",
      "exampleValue" : ""
    }
  }
}
```

IncrementLoginCount

Realm Operations

Resource path: `/realm-config/authentication/authenticationtrees/nodes/IncrementLoginCountNode`

Resource version: `1.0`

create

Usage:

```
am> create IncrementLoginCount --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "identityAttribute" : {
      "title" : "Identity Attribute",
      "description" : "The attribute of the IDM object to use retrieve the object.",
      "propertyOrder" : 100,
      "type" : "string",
      "exampleValue" : ""
    }
  },
  "required" : [ "identityAttribute" ]
}
```

delete

Usage:

```
am> delete IncrementLoginCount --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action IncrementLoginCount --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action IncrementLoginCount --realm Realm --actionName getCreatableTypes
```

listOutcomes

List the available outcomes for the node type.

Usage:

```
am> action IncrementLoginCount --realm Realm --body body --actionName listOutcomes
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "title" : "Some configuration of the node. This does not need to be complete against the
 configuration schema."
}
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action IncrementLoginCount --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query IncrementLoginCount --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read IncrementLoginCount --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update IncrementLoginCount --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "identityAttribute" : {
      "title" : "Identity Attribute",
      "description" : "The attribute of the IDM object to use retrieve the object.",
      "propertyOrder" : 100,
      "type" : "string",
      "exampleValue" : ""
    }
  },
  "required" : [ "identityAttribute" ]
}
```

InnerTreeEvaluator

Realm Operations

Resource path: `/realm-config/authentication/authenticationtrees/nodes/InnerTreeEvaluatorNode`

Resource version: `1.0`

create

Usage:

```
am> create InnerTreeEvaluator --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "tree" : {
      "title" : "Tree Name",
      "description" : "The name of the tree that will be evaluated.",
      "propertyOrder" : 100,
      "type" : "string",
      "exampleValue" : ""
    }
  },
  "required" : [ "tree" ]
}
```

delete

Usage:

```
am> delete InnerTreeEvaluator --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action InnerTreeEvaluator --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action InnerTreeEvaluator --realm Realm --actionName getCreatableTypes
```

listOutcomes

List the available outcomes for the node type.

Usage:

```
am> action InnerTreeEvaluator --realm Realm --body body --actionName listOutcomes
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "title" : "Some configuration of the node. This does not need to be complete against the
 configuration schema."
}
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action InnerTreeEvaluator --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query InnerTreeEvaluator --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read InnerTreeEvaluator --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update InnerTreeEvaluator --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "tree" : {
      "title" : "Tree Name",
      "description" : "The name of the tree that will be evaluated.",
      "propertyOrder" : 100,
      "type" : "string",
      "exampleValue" : ""
    }
  },
  "required" : [ "tree" ]
}
```

IoTService

Realm Operations

Resource path: `/realm-config/services/iot`

Resource version: `1.0`

create

Usage:

```
am> create IoTService --realm Realm --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "oauthJwtIssuerName" : {
      "title" : "OAuth 2.0 JWT Issuer Name",
      "description" : "The name of the Trusted JWT Issuer used by the IoT Service to request access
 tokens for things.",
      "propertyOrder" : 40,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "attributeAllowlist" : {
      "title" : "Readable Attributes",
      "description" : "Specifies the list of attributes that a thing is allowed to request from its
 identity.",
      "propertyOrder" : 50,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "createOAuthClient" : {
      "title" : "Create OAuth 2.0 Client",
      "description" : "Create an OAuth 2.0 Client with the given name and default configuration
 required to serve as the client for the IoT Service. The client will be created without any
 scope(s).",
      "propertyOrder" : 10,
      "required" : true,
      "type" : "boolean",
```

```
      "exampleValue" : ""
    },
    "createOAuthJwtIssuer" : {
      "title" : "Create OAuth 2.0 JWT Issuer",
      "description" : "Create a Trusted JWT Issuer with the given name and default configuration
 required for the IoT Service to act as the Issuer when handling request for thing access tokens.",
      "propertyOrder" : 30,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "oauthClientName" : {
      "title" : "OAuth 2.0 Client Name",
      "description" : "The name of the default OAuth 2.0 Client used by the IoT Service to request
 access tokens for things.",
      "propertyOrder" : 20,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
```

delete

Usage:

```
am> delete IoTService --realm Realm
```

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action IoTService --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action IoTService --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action IoTService --realm Realm --actionName nextdescendents
```

read

Usage:

```
am> read IoTService --realm Realm
```

update

Usage:

```
am> update IoTService --realm Realm --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "oauthJwtIssuerName" : {
      "title" : "OAuth 2.0 JWT Issuer Name",
      "description" : "The name of the Trusted JWT Issuer used by the IoT Service to request access
 tokens for things.",
      "propertyOrder" : 40,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "attributeAllowlist" : {
      "title" : "Readable Attributes",
      "description" : "Specifies the list of attributes that a thing is allowed to request from its
 identity.",
      "propertyOrder" : 50,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "createOAuthClient" : {
      "title" : "Create OAuth 2.0 Client",
      "description" : "Create an OAuth 2.0 Client with the given name and default configuration
 required to serve as the client for the IoT Service. The client will be created without any
 scope(s).",
      "propertyOrder" : 10,
      "required" : true,
      "type" : "boolean",
```

```
      "exampleValue" : ""
    },
    "createOAuthJwtIssuer" : {
      "title" : "Create OAuth 2.0 JWT Issuer",
      "description" : "Create a Trusted JWT Issuer with the given name and default configuration
 required for the IoT Service to act as the Issuer when handling request for thing access tokens.",
      "propertyOrder" : 30,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "oauthClientName" : {
      "title" : "OAuth 2.0 Client Name",
      "description" : "The name of the default OAuth 2.0 Client used by the IoT Service to request
 access tokens for things.",
      "propertyOrder" : 20,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
```

Global Operations

Resource path: `/global-config/services/iot`

Resource version: `1.0`

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action IoTService --global --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action IoTService --global --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action IoTService --global --actionName nextdescendents
```

read

Usage:

```
am> read IoTService --global
```

update

Usage:

```
am> update IoTService --global --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "defaults" : {
      "properties" : {
        "oauthClientName" : {
          "title" : "OAuth 2.0 Client Name",
          "description" : "The name of the default OAuth 2.0 Client used by the IoT Service to request
 access tokens for things.",
          "propertyOrder" : 20,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "createOAuthJwtIssuer" : {
          "title" : "Create OAuth 2.0 JWT Issuer",
          "description" : "Create a Trusted JWT Issuer with the given name and default configuration
 required for the IoT Service to act as the Issuer when handling request for thing access tokens.",
          "propertyOrder" : 30,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "oauthJwtIssuerName" : {
          "title" : "OAuth 2.0 JWT Issuer Name",
          "description" : "The name of the Trusted JWT Issuer used by the IoT Service to request
 access tokens for things.",
          "propertyOrder" : 40,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
```

```
        "attributeAllowlist" : {
          "title" : "Readable Attributes",
          "description" : "Specifies the list of attributes that a thing is allowed to request from
 its identity.",
          "propertyOrder" : 50,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "createOAuthClient" : {
          "title" : "Create OAuth 2.0 Client",
          "description" : "Create an OAuth 2.0 Client with the given name and default configuration
 required to serve as the client for the IoT Service. The client will be created without any
 scope(s).",
          "propertyOrder" : 10,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        }
      },
      "type" : "object",
      "title" : "Realm Defaults"
    }
  }
}
```

J2EEAgentGroups

Realm Operations

Agent Groups handler that is responsible for managing agent groups

Resource path: `/realm-config/agents/groups/J2EEAgent`

Resource version: `1.0`

create

Usage:

```
am> create J2EEAgentGroups --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "applicationJ2EEAgentConfig" : {
      "type" : "object",
      "title" : "Application",
      "propertyOrder" : 1,
      "properties" : {
        "notEnforcedFavicon" : {
          "title" : "Not Enforced Favicon",
          "description" : "This flag, if enabled, automatically adds \"*/favicon.ico\" to
the not enforced list.  This can help to avoid odd situations in which a user is required to
log in after logging out, just because favicon.ico has been requested by browser. (property:
org.forgerock.agents.auto.not.enforce.favicon.enabled) <br>Required Agent Restart",
          "propertyOrder" : 7650,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "continuousSecurityHeaders" : {
          "title" : "Continuous Security Headers",
          "description" : "The name of the headers in the user's original request, that will be sent
as part of the payload during policy evaluation, which can then be accessed via the 'environment'
variable in a policy script. The 'key' is the name of the header to be sent, and the 'value' is the
name which it will appear as in the policy evaluation script.It is possible to map multiple headers
to the same name (they will simply appear as an array in the evaluation script). If the header
doesn't exist, then the empty string will be sent.",
          "propertyOrder" : 3211,
          "required" : false,
          "patternProperties" : {
            ".*" : {
              "type" : "string"
            }
          },
          "type" : "object",
          "exampleValue" : ""
        },
        "resourceAccessDeniedUri" : {
          "title" : "Resource Access Denied URI",
          "description" : "An application-specific Map that identifies a URI of the customized access
denied page. (property name: org.forgerock.agents.access.denied.uri.map) <br>Valid key: the web
application name. <br>Valid value: the customized application access denied page URI. <br>For this
property, a global value can be set to apply to all the applications that don't have their own
specific access denied page.  <br> Examples: <br>To set a global access denied page: leave Map Key
field empty, and enter the global access denied page URI /sample/accessdenied.html in Corresponding
Map Value field. <br> To set the access denied page URI for application BankApp: enter BankApp
in Map Key field, and enter the application access denied page URI /BankApp/accessdenied.html in
Corresponding Map Value field.",
          "propertyOrder" : 2700,
          "required" : false,
          "patternProperties" : {
            ".*" : {
              "type" : "string"
            }
          },
```

```
          "type" : "object",
          "exampleValue" : ""
        },
        "cookieAttributeUrlEncoded" : {
          "title" : "Attribute Cookie Encode",
          "description" : "Indicates if the value of the attribute should be URL encoded before being
set as a cookie. (property name: org.forgerock.agents.attribute.cookie.encode.enabled) ",
          "propertyOrder" : 8500,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "profileAttributeFetchMode" : {
          "title" : "Profile Attribute Fetch Mode",
          "description" : "The mode of fetching profile attributes. (property name:
com.sun.identity.agents.config.profile.attribute.fetch.mode) ",
          "propertyOrder" : 8700,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "notEnforcedIps" : {
          "title" : "Not Enforced Client IP List",
          "description" : "No authentication and authorization protection from agent
are required for the requests coming from these client IP addresses. (property name:
org.forgerock.agents.notenforced.ip.list)  <br> Examples: <br> 192.18.145.* <br> 192.18.146.123",
          "propertyOrder" : 7900,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "cookieAttributeMultiValueSeparator" : {
          "title" : "Cookie Separator Character",
          "description" : "Character that will be used to separate multiple
values of the same attribute when it is being set as a cookie. (property name:
org.forgerock.agents.attribute.cookie.separator) ",
          "propertyOrder" : 8300,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "continuousSecurityCookies" : {
          "title" : "Continuous Security Cookies",
          "description" : "The name of the cookies to be sent as part of the payload during policy
evaluation, which can be accessed via the 'environment' variable in a policy script. The 'key' is
the name of the cookie to be sent, and the 'value' is the name which it will appear as in the policy
evaluation script. It is possible to map multiple cookies to the same name (they will simply appear
as an array in the evaluation script). If the cookie doesn't exist, then the empty string will be
sent.",
          "propertyOrder" : 3210,
          "required" : false,
          "patternProperties" : {
            ".*" : {
              "type" : "string"
            }
          },
```

```
          "type" : "object",
          "exampleValue" : ""
        },
        "profileAttributeMap" : {
          "title" : "Profile Attribute Mapping",
          "description" : "Maps the profile attributes to be populated under specific names for the
 currently authenticated user. (property name: org.forgerock.agents.profile.attribute.map)  <br>
 Example: <br> To populate the value of profile attribute cn under name CUSTOM-Common-Name: enter cn
 in Map Key field, and enter CUSTOM-Common-Name in Corresponding Map Value field. <br> To populate
 the value of profile attribute mail under name CUSTOM-Email: enter mail in Map Key field, and enter
 CUSTOM-Email in Corresponding Map Value field.",
          "propertyOrder" : 8800,
          "required" : false,
          "patternProperties" : {
            ".*" : {
              "type" : "string"
            }
          },
          "type" : "object",
          "exampleValue" : ""
        },
        "notEnforcedIpsCacheSize" : {
          "title" : "Not Enforced IP Cache Size",
          "description" : "Size of the cache to be used if Not Enforced IP Cache Flag is enabled.
 (property name: org.forgerock.agents.notenforced.ip.cache.size) ",
          "propertyOrder" : 8200,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "notEnforcedUrisCacheEnabled" : {
          "title" : "Not Enforced URIs Cache Enabled",
          "description" : "Enables the caching of the Not Enforced URIs list evaluation results.
 (property name: org.forgerock.agents.notenforced.uri.cache.enabled) ",
          "propertyOrder" : 7700,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "notEnforcedUris" : {
          "title" : "Not Enforced URIs",
          "description" : "List of URIs for which protection is not enforced by the Agent. (property
 name: org.forgerock.agents.notenforced.uri.list)  <br> Examples: <br> /BankApp/public/* <br> /
BankApp/images/*",
          "propertyOrder" : 7500,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "logoutIntrospection" : {
          "title" : "Logout Introspect Enabled",
          "description" : "Allows the Agent to search HTTP request body to locate logout parameter.
 (property name: org.forgerock.agents.logout.introspection.enabled) ",
          "propertyOrder" : 6200,
          "required" : false,
          "type" : "boolean",
```

```
          "exampleValue" : ""
        },
        "responseAttributeFetchMode" : {
          "title" : "Response Attribute Fetch Mode",
          "description" : "The mode of fetching policy response attributes. (property name:
 com.sun.identity.agents.config.response.attribute.fetch.mode) ",
          "propertyOrder" : 9100,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "responseAttributeMap" : {
          "title" : "Response Attribute Mapping",
          "description" : "Maps the policy response attributes to be populated under specific names
 for the currently authenticated user. (property name: org.forgerock.agents.response.attribute.map)
 <br> Example: <br> To populate the value of response attribute uid under name CUSTOM-USER-NAME: enter
 uid in Map Key field, and enter CUSTOM-USER-NAME in Corresponding Map Value field.",
          "propertyOrder" : 9200,
          "required" : false,
          "patternProperties" : {
            ".*" : {
              "type" : "string"
            }
          },
          "type" : "object",
          "exampleValue" : ""
        },
        "logoutEntryUri" : {
          "title" : "Logout Entry URI",
          "description" : "An application-specific Map that identifies a URI to be used as an entry
 point after successful logout and subsequent successful authentication if applicable. (property name:
 org.forgerock.agents.logout.goto.map) <br>Valid key: the web application name. <br>Valid value: the
 logout entry URI. <br>For this property, a global value can be set to apply to all the applications
 that don't have their own specific logout entry URI.   <br> Examples: <br>To set a global application
 logout entry URI: leave Map Key field empty, and enter the global application logout entry URI /
welcome.html in Corresponding Map Value field. <br> To set the logout entry URI for application
 BankApp: enter BankApp in Map Key field, and enter the logout entry URI /BankApp/welcome.html in
 Corresponding Map Value field.",
          "propertyOrder" : 6300,
          "required" : false,
          "patternProperties" : {
            ".*" : {
              "type" : "string"
            }
          },
          "type" : "object",
          "exampleValue" : ""
        },
        "sessionAttributeFetchMode" : {
          "title" : "Session Attribute Fetch Mode",
          "description" : "The mode of fetching session attributes. (property name:
 com.sun.identity.agents.config.session.attribute.fetch.mode) ",
          "propertyOrder" : 8900,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "applicationLogoutUris" : {
          "title" : "Application Logout URI",
```

```
          "description" : "An application-specific Map that identifies a request URI which indicates
 a logout event. (property name: org.forgerock.agents.logout.endpoint.map) <br>Valid key: the web
 application name. <br>Valid value: the application logout URI. <br>For this property, a global value
 can be set to apply to all the applications that don't have their own specific logout URI.  <br>
 Examples: <br>To set a global application logout URI: leave Map Key field empty, and enter the global
 application logout URI /logout.jsp in Corresponding Map Value field. <br> To set the logout URI for
 application BankApp: enter BankApp in Map Key field, and enter the application logout URI /BankApp/
logout.jsp in Corresponding Map Value field.",
          "propertyOrder" : 6000,
          "required" : false,
          "patternProperties" : {
            ".*" : {
              "type" : "string"
            }
          },
          "type" : "object",
          "exampleValue" : ""
        },
        "notEnforcedIpsCacheEnabled" : {
          "title" : "Not Enforced IP Cache Flag",
          "description" : "Enable caching of not-enforced IP list evaluation results. (property name:
 org.forgerock.agents.notenforced.ip.cache.enabled) ",
          "propertyOrder" : 8100,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "headerAttributeDateFormat" : {
          "title" : "Fetch Attribute Date Format",
          "description" : "Format of date attribute values to be used when the attribute is
 being set as HTTP header. Format is based on java.text.SimpleDateFormat. (property name:
 org.forgerock.agents.attribute.date.format) ",
          "propertyOrder" : 8400,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "notEnforcedUrisCacheSize" : {
          "title" : "Not Enforced URIs Cache Size",
          "description" : "Size of the cache to be used if caching of not enforced URI list evaluation
 results is enabled. (property name: org.forgerock.agents.notenforced.uri.cache.size) ",
          "propertyOrder" : 7800,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "sessionAttributeMap" : {
          "title" : "Session Attribute Mapping",
          "description" : "Maps the session attributes to be populated under specific names for the
 currently authenticated user. (property name: org.forgerock.agents.session.attribute.map)   <br>
 Example: <br>  To populate the value of session attribute UserToken under name CUSTOM-userid: enter
 UserToken in Map Key field, and enter CUSTOM-userid in Corresponding Map Value field.",
          "propertyOrder" : 9000,
          "required" : false,
          "patternProperties" : {
            ".*" : {
              "type" : "string"
            }
          },
```

```
          "type" : "object",
          "exampleValue" : ""
        },
        "logoutRequestParameters" : {
          "title" : "Logout Request Parameter",
          "description" : "An application-specific Map that identifies a parameter
 which when present in the HTTP request indicates a logout event. (property name:
 org.forgerock.agents.logout.request.param.map)  <br>Valid key: the web application name. <br>Valid
 value: the logout request parameter. <br>For this property, a global value can be set to apply to
 all the applications that don't have their own specific logout request parameter.   <br> Examples:
 <br>To set a global application logout request parameter: leave Map Key field empty, and enter the
 global application logout request parameter logoutparam in Corresponding Map Value field. <br> To set
 the logout request parameter for application BankApp: enter BankApp in Map Key field, and enter the
 logout request parameter logoutparam in Corresponding Map Value field.",
          "propertyOrder" : 6100,
          "required" : false,
          "patternProperties" : {
            ".*" : {
              "type" : "string"
            }
          },
          "type" : "object",
          "exampleValue" : ""
        },
        "loginFormUri" : {
          "title" : "Login Form URI",
          "description" : "List of absolute URIs corresponding to an application's web.xml form-login-
page element. (property name: com.sun.identity.agents.config.login.form)  <br> Example: <br> /BankApp/
jsp/login.jsp",
          "propertyOrder" : 2800,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "invertNotEnforcedIps" : {
          "title" : "Invert Not Enforced IPs",
          "description" : "Client IP Addresses to invert protection of IP
 addresses listed in the related Not Enforced Client IP List. (property name:
 org.forgerock.agents.notenforced.ip.invert.enabled) ",
          "propertyOrder" : 8000,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "invertNotEnforcedUris" : {
          "title" : "Invert Not Enforced URIs",
          "description" : "Inverts protection of  URIs specified in Not Enforced URIs list. When set
 to true, it indicates that the URIs specified should be enforced and all other URIs should be not
 enforced by the Agent. (property name: org.forgerock.agents.notenforced.uri.invert.enabled) ",
          "propertyOrder" : 7600,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "notEnforcedRuleCompoundSeparator" : {
          "title" : "Not Enforced Compound Rule Separator",
```

```
          "description" : "Specifies a separator for not enforced compound rules. The format for
compound rules requires a list of IP rules, a separator (by default the | character), and a list of
URI rules. <br>Example, GET 192.168.1.1-192.168.4.3 | /images/* <br>Configure a different separator
(for example, &&) when working with the REGEX keyword to avoid invalid regular expressions.",
          "propertyOrder" : 7450,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "globalJ2EEAgentConfig" : {
      "type" : "object",
      "title" : "Global",
      "propertyOrder" : 0,
      "properties" : {
        "localAuditRotationSize" : {
          "title" : "Local Audit Log Rotation Size",
          "description" : "Size limit when a local audit log file is rotated to a new file. (property
name: com.sun.identity.agents.config.local.log.size) ",
          "propertyOrder" : 1900,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "debugLogfileSuffix" : {
          "title" : "Debug File Rotation Suffix",
          "description" : "This is a value appended onto the end of the debug file name when it is
rotated. The user is free to define it as they want, but if it does not involve a timestamp that
produces different file names when the rotation time is reached, log file rotation is unlikely to
function correctly (property: org.forgerock.agents.debug.suffix)",
          "propertyOrder" : 10020,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "cdssoRootUrl" : {
          "title" : "Agent Root URL for CDSSO",
          "description" : "The agent root URL for CDSSO. The valid value is in the following format:
<br>protocol://hostname:port/<br> The protocol represents the protocol used, such as http or https.
The hostname represents the host name of the machine on which the agent resides. The port represents
the port number on which the agent is installed. The slash following the port number is required.",
          "propertyOrder" : 22700,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "localAuditLogfilePath" : {
          "title" : "Audit Logfile Path",
          "description" : "The full path of the local auditing file. (property:
org.forgerock.agents.local.audit.file.path)",
          "propertyOrder" : 2000,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
```

```
       "localAuditLogRotation" : {
         "title" : "Rotate Local Audit Log",
         "description" : "Flag to indicate that audit log files should be rotated when reaching a
certain size. (property name: org.forgerock.agents.local.audit.log.rotation.enabled) ",
         "propertyOrder" : 1800,
         "required" : false,
         "type" : "boolean",
         "exampleValue" : ""
       },
       "debugLogfileDirectory" : {
         "title" : "Debug Logfile Directory",
         "description" : "Location of the agent logs files, and where monitoring CSV files are
written. This is normally set in bootstrap properties during the install process. Note there is no
default and no logging will occur until a value for this property is provided. Anything logged will
be written to the standard output and may end up in the container log file (so \"catalina.out\" in
the case of Tomcat). (property: org.forgerock.agents.csv.monitoring.directory)",
         "propertyOrder" : 10060,
         "required" : false,
         "type" : "string",
         "exampleValue" : ""
       },
       "configurationReloadInterval" : {
         "title" : "Configuration Reload Interval",
         "description" : "Only used when websocket notifications are disabled, specifies
interval in seconds after which config is reloaded automatically by the Agent. (property name:
org.forgerock.agents.config.reload.seconds) ",
         "propertyOrder" : 1200,
         "required" : false,
         "type" : "integer",
         "exampleValue" : ""
       },
       "loginAttemptLimitCookieName" : {
         "title" : "Login Attempt Limit Cookie Name",
         "description" : "The name of the cookie used to record the number of login attempts.
(property: org.forgerock.agents.login.counter.cookie.name)",
         "propertyOrder" : 4500,
         "required" : false,
         "type" : "string",
         "exampleValue" : ""
       },
       "fallforwardModeEnabled" : {
         "title" : "Fall-Forward Mode",
         "description" : "This property is used when AM is not available. <br>  Disabled: the
Agent will deny every incoming request with an HTTP 403 <br>  Enabled: the Agent will continue
to allow access to any resource matched by a not enforced rule until AM becomes available again
<br><br>(property: org.forgerock.agents.session.change.notifications.enabled) (Agent 5.7+ only)",
         "propertyOrder" : 12115,
         "required" : false,
         "type" : "boolean",
         "exampleValue" : ""
       },
       "debugLogfileRotationMinutes" : {
         "title" : "Debug File Rotation Time",
         "description" : "This is the time in minutes after which log file rotation will occur.
(property: org.forgerock.agents.debug.rotation.time.minutes)",
         "propertyOrder" : 10040,
         "required" : false,
         "type" : "integer",
         "exampleValue" : ""
```

```
      },
      "auditLogLocation" : {
        "title" : "Audit Log Location",
        "description" : "LOCAL = audit information stored in files based locally
to the Agent container <br>REMOTE = audit information logged via AM. (property name:
org.forgerock.agents.audit.where) ",
        "propertyOrder" : 1600,
        "required" : false,
        "type" : "string",
        "exampleValue" : ""
      },
      "loginAttemptLimit" : {
        "title" : "Login Attempt Limit",
        "description" : "Limit of failed login attempts for a user's single browser session until
triggering the blocking of the user request. Value of 0 disables this feature. (property name:
org.forgerock.agents.login.attempt.limit.count) ",
        "propertyOrder" : 4400,
        "required" : false,
        "type" : "integer",
        "exampleValue" : ""
      },
      "debugLogfilePrefix" : {
        "title" : "Debug File Rotation Prefix",
        "description" : "Prefix which can be added onto the front of the debug file name when it is
rotated. (property: org.forgerock.agents.debug.prefix)",
        "propertyOrder" : 10010,
        "required" : false,
        "type" : "string",
        "exampleValue" : ""
      },
      "debugLogfileRetentionCount" : {
        "title" : "Debug File Rotation Retention Count",
        "description" : "This is the number of log files to retain after rotation, so for example,
setting it to 10 would give you one current debug file and nine older (rotated) files. (property:
org.forgerock.agents.debug.retention.count)",
        "propertyOrder" : 10050,
        "required" : false,
        "type" : "integer",
        "exampleValue" : ""
      },
      "redirectAttemptLimit" : {
        "title" : "Redirect Attempt Limit",
        "description" : "Number of successive single point redirects that a user can make using a
single browser session which will trigger the blocking of the user request. Set to 0 to disable this
feature. (property name: org.forgerock.agents.redirect.attempt.limit) ",
        "propertyOrder" : 7100,
        "required" : false,
        "type" : "integer",
        "exampleValue" : ""
      },
      "redirectAttemptLimitCookieName" : {
        "title" : "Redirect Attempt Cookie Name",
        "description" : "Agent tries to detect redirect loops while authenticating, which would
normally indicate a cookie domain problem.  The Agent does this by using a cookie to holds the
current redirection count. (property: org.forgerock.agents.redirect.cookie.name)",
        "propertyOrder" : 7150,
        "required" : false,
        "type" : "string",
        "exampleValue" : ""
```

```
      },
      "customResponseHeader" : {
        "title" : "Custom Response Header",
        "description" : "Map specifies the custom headers that are set by the Agent on the client
browser. The key is the header name and the value represents the header value. (property name:
org.forgerock.agents.response.header.map)  <br> Example: <br>  To set the custom header Cache-Control
to value no-cache: enter Cache-Control in Map Key field, and enter no-cache in Corresponding Map
Value field.",
        "propertyOrder" : 7000,
        "required" : false,
        "patternProperties" : {
          ".*" : {
            "type" : "string"
          }
        },
        "type" : "object",
        "exampleValue" : ""
      },
      "filterMode" : {
        "title" : "Agent Filter Mode",
        "description" : "Specifies the mode of operation of the Filter. (property name:
org.forgerock.agents.filter.mode.map) <br>Valid key: the web application name. <br>Valid values:
ALL, URL_POLICY, SSO_ONLY, NONE <br>For this property, a global value can be set to apply to all
the applications that don't have their own specific filter mode. <br>Examples: <br>To set ALL as the
global filter mode: leave Map Key field empty, and enter ALL in Corresponding Map Value field. <br>To
set URL_POLICY as the filter mode for application BankApp: enter BankApp in Map Key field, and enter
URL_POLICY in Corresponding Map Value field.",
        "propertyOrder" : 500,
        "required" : false,
        "patternProperties" : {
          ".*" : {
            "type" : "string"
          }
        },
        "type" : "object",
        "exampleValue" : ""
      },
      "userPrincipalFlag" : {
        "title" : "User Principal Flag",
        "description" : "Use principal instead of just the user-ID for authenticating the user.
(property name: org.forgerock.agents.userid.mapping.mode.use.dn.enabled) ",
        "propertyOrder" : 800,
        "required" : false,
        "type" : "boolean",
        "exampleValue" : ""
      },
      "userTokenName" : {
        "title" : "User Token Name",
        "description" : "Session property name for user-ID of the authenticated user in session.
(property name: org.forgerock.agents.userid.mapping.mode.use.session.property.name) ",
        "propertyOrder" : 900,
        "required" : false,
        "type" : "string",
        "exampleValue" : ""
      },
      "fqdnCheck" : {
        "title" : "FQDN Check",
        "description" : "Enables checking of fqdn default value and fqdn map values. (property name:
org.forgerock.agents.fqdn.check.enabled) ",
```

```
          "propertyOrder" : 6400,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "preAuthCookieName" : {
          "title" : "Pre-Authenticated Cookie Name",
          "description" : "Specifies the name of the cookie the agent uses to track the progress of
authentication with AM. (property: org.forgerock.agents.authn.cookie.name)",
          "propertyOrder" : 11210,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "preAuthCookieMaxAge" : {
          "title" : "Pre-Authenticated Cookie Max Age",
          "description" : "This is the amount of time in seconds before the pre-authn cookie will
timeout. (property: org.forgerock.agents.authn.cookie.max.age.seconds)",
          "propertyOrder" : 11220,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "agentSessionChangeNotificationsEnabled" : {
          "title" : "Session Logout Notification ",
          "description" : "Flag to indicate whether the Agent will subscribe
to session logout notifications (via websockets) from AM. (property:
org.forgerock.agents.session.change.notifications.enabled)",
          "propertyOrder" : 12110,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "userAttributeName" : {
          "title" : "User Attribute Name",
          "description" : "Name of the attribute which contains the user-ID. (property name:
org.forgerock.agents.user.mapping.mode.attribute.name) ",
          "propertyOrder" : 700,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "auditAccessType" : {
          "title" : "Audit Access Types",
          "description" : "Types of messages to log based on user URL access attempts. (property name:
org.forgerock.agents.audit.what) ",
          "propertyOrder" : 1500,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "debugLogfileRotationSize" : {
          "title" : "Debug File Rotation Size",
          "description" : "This specifies the approximate size in bytes at which a log file will be
rotated to a new log file. (property: org.forgerock.agents.debug.rotation.size.bytes)",
          "propertyOrder" : 10030,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
```

```
      },
      "localAuditLogfileRetentionCount" : {
        "title" : "Audit Logfile Retention Count",
        "description" : "The number of audit log files to retain after rotation has occurred.
(property: org.forgerock.agents.local.audit.log.retention.count)",
        "propertyOrder" : 2100,
        "required" : false,
        "type" : "integer",
        "exampleValue" : ""
      },
      "httpSessionBinding" : {
        "title" : "HTTP Session Binding",
        "description" : "If true will invalidate the http session when login has failed,
user has no SSO session, or principal user name does not match SSO user name. (property name:
org.forgerock.agents.http.session.binding.enabled) ",
        "propertyOrder" : 3500,
        "required" : false,
        "type" : "boolean",
        "exampleValue" : ""
      },
      "fqdnMapping" : {
        "title" : "FQDN Virtual Host Map",
        "description" : "Maps virtual, invalid, or partial hostnames, and IP addresses to the
FQDN to access protected resources. (property name: org.forgerock.agents.fqdn.map)  <br> Examples:
<br>  To map the partial hostname myserver to myserver.mydomain.com: enter myserver in the Map
Key field and myserver.mydomain.com in the Corresponding Map Value field. To map a virtual server
rst.hostname.com that points to the actual server abc.hostname.com: enter valid1 in the Map Key field
and rst.hostname.com in the Corresponding Map Value field.",
        "propertyOrder" : 6600,
        "required" : false,
        "patternProperties" : {
          ".*" : {
            "type" : "string"
          }
        },
        "type" : "object",
        "exampleValue" : ""
      },
      "jwtName" : {
        "title" : "JWT Cookie Name",
        "description" : "The name used by the agent to set the OIDC JWT on the user's browser.
(property: org.forgerock.agents.jwt.cookie.name)",
        "propertyOrder" : 11201,
        "required" : false,
        "type" : "string",
        "exampleValue" : ""
      },
      "agentConfigChangeNotificationsEnabled" : {
        "title" : "Agent Configuration Change Notification",
        "description" : "Enable agent to receive notification messages
(via websockets) from AM server for configuration changes. (property name:
org.forgerock.agents.config.change.notifications.enabled) ",
        "propertyOrder" : 12100,
        "required" : false,
        "type" : "boolean",
        "exampleValue" : ""
      },
      "debugLevel" : {
        "title" : "Agent Debug Level",
```

```
          "description" : "Specifies type of agent debug messages to log. (property name:
com.iplanet.services.debug.level) ",
          "propertyOrder" : 10000,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "status" : {
          "title" : "Status",
          "description" : "Status of the agent configuration.",
          "propertyOrder" : 200,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "webSocketConnectionIntervalInMinutes" : {
          "title" : "Web Socket Connection Interval",
          "description" : "Interval in minutes by which agents reopen their web socket
connection to ensure a fair distribution of connections across AM servers. (property:
org.forgerock.agents.balance.websocket.interval.minutes).",
          "propertyOrder" : 12120,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "userMappingMode" : {
          "title" : "User Mapping Mode",
          "description" : "Specifies mechanism agent uses to determine user-ID. (property name:
org.forgerock.agents.user.mapping.mode) ",
          "propertyOrder" : 600,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "fqdnDefault" : {
          "title" : "FQDN Default",
          "description" : "Fully qualified hostname that the users should use in order to access
resources. (property name: org.forgerock.agents.fqdn.default) ",
          "propertyOrder" : 6500,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "miscJ2EEAgentConfig" : {
      "type" : "object",
      "title" : "Miscellaneous",
      "propertyOrder" : 4,
      "properties" : {
        "portCheckFile" : {
          "title" : "Port Check File",
          "description" : "Name or complete path of a file that has the necessary content needed to
handle requests that need port correction. (property name: org.forgerock.agents.port.check.file) ",
          "propertyOrder" : 7300,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
```

```
        "loginReasonMap" : {
          "title" : "Login Reason Value Map",
          "description" : "This map allows some of the possible reasons to be mapped to
 arbitrary values, when empty will be used default values(see: \"Login Reason Parameter Name
\" description). LOGIN REASON=CUSTOM VALUE e.g. [JWT_INVALID]=corrupted_token. (property:
 org.forgerock.agents.login.reason.remapper)",
          "propertyOrder" : 18800,
          "required" : false,
          "patternProperties" : {
            ".*" : {
              "type" : "string"
            }
          },
          "type" : "object",
          "exampleValue" : ""
        },
        "ignorePathInfo" : {
          "title" : "Ignore Path Info in Request URL",
          "description" : "The path info will be stripped from the request URL while doing Not
 Enforced List check and url policy evaluation if the value is set to true. (property name:
 com.sun.identity.agents.config.ignore.path.info)",
          "propertyOrder" : 18600,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "legacyRedirectUri" : {
          "title" : "Legacy User Agent Redirect URI",
          "description" : "An intermediate URI used by the Agent to redirect legacy user agent
 requests. (property name: org.forgerock.agents.legacy.redirect.uri) ",
          "propertyOrder" : 6900,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "authFailReasonParameterName" : {
          "title" : "Authentication Fail Reason Parameter Name",
          "description" : "If this property is defined, the agent will pass the named parameter
 to a custom page (defined by \"Authentication Fail Reason Url\") saying why authentication
 failed.  The reason can be very detailed and users may want to use the \"Authentication
 Fail Reason Parameter Value Map\" to give custom detail, otherwise these default values
 will be used: AUTHN_BOOKKEEPING_COOKIE_MISSING, NONCE_MISSING, EXCEPTION (property:
 org.forgerock.agents.authn.fail.reason.parameter.name)",
          "propertyOrder" : 19000,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "wantedHttpUrlRegexParams" : {
          "title" : "Regular Expression Retain Query Parameters",
          "description" : "Specifies a list of regular expressions the agent uses to match query
 parameters to be retained for policy decision and caching purposes. The property has the format
 [Domain/path] | regular_expression[,regular_expression...] with no spaces between values. (property:
 org.forgerock.agents.wanted.http.url.params.regex.list)",
          "propertyOrder" : 19400,
          "required" : false,
          "items" : {
            "type" : "string"
          },
```

```
          "type" : "array",
          "exampleValue" : ""
        },
        "gotoParameterName" : {
          "title" : "Goto Parameter Name",
          "description" : "This is the name of the HTTP query \"goto\" parameter. It is not
recommended to change it. (property name: com.sun.identity.agents.config.redirect.param) ",
          "propertyOrder" : 3600,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "gotoUrl" : {
          "title" : "Goto Url",
          "description" : "This is a URL used in rare circumstances where the Agent has nowhere
else to go.  For instance if the user requests a resource, authenticates for the first time,
then presses the back button and the administrator hasn't set up the authn fail URL. (property:
org.forgerock.agents.default.goto.url)",
          "propertyOrder" : 19200,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "unwantedHttpUrlParams" : {
          "title" : "Remove Query Parameters",
          "description" : "Specifies a list of query parameters to be removed from a URL for policy
decision and caching purposes. The property has the format [Domain/path] | parameter[,parameter...]
with no spaces between values (property: org.forgerock.agents.unwanted.http.url.param.list)
<br>Example: myapp.example.com/customers|location,lang",
          "propertyOrder" : 19500,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "serviceResolverClass" : {
          "title" : "Service Resolver Class Name",
          "description" : "Name of the service resolver class to change in order
to instantiate own service resolver and overriding default ones <br>(property:
org.forgerock.agents.service.resolver.class.name) (Agent 5.6.2+ only) <br> Agent restart is
required",
          "propertyOrder" : 19700,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "authFailReasonParameterRemapper" : {
          "title" : "Authentication Fail Reason Parameter Value Map",
          "description" : "This map allows some of the possible reasons to be
mapped to arbitrary values. When empty, will use default values. (property:
org.forgerock.agents.authn.fail.reason.remapper)",
          "propertyOrder" : 19100,
          "required" : false,
          "patternProperties" : {
            ".*" : {
              "type" : "string"
            }
```

```
          },
          "type" : "object",
          "exampleValue" : ""
        },
        "legacyUserAgentSupport" : {
          "title" : "Legacy User Agent Support Enable",
          "description" : "Enables support for legacy user agents (browser). (property name:
 org.forgerock.agents.legacy.support.enabled) ",
          "propertyOrder" : 6700,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "portCheckSetting" : {
          "title" : "Port Check Setting",
          "description" : "Map of port versus protocol entries with the key being the listening port
 number and value being the listening protocol to be used by the Agent to identify requests with
 invalid port numbers. (property name: org.forgerock.agents.port.check.map)  <br> Example: <br> To
 map port 80 to protocol http: enter 80 in Map Key field, and enter http in Corresponding Map Value
 field.",
          "propertyOrder" : 7400,
          "required" : false,
          "patternProperties" : {
            ".*" : {
              "type" : "string"
            }
          },
          "type" : "object",
          "exampleValue" : ""
        },
        "wantedHttpUrlParams" : {
          "title" : "Retain Query Parameters",
          "description" : "Specifies a list of query parameters to be retained (other parameters
 will be removed) from a URL for policy decision and caching purposes. The property has the
 format [Domain/path] | parameter[,parameter...] with no spaces between values. (property:
 org.forgerock.agents.wanted.http.url.param.list) <br>Example: myapp.example.com/customers|
location,lang",
          "propertyOrder" : 19300,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "portCheckEnabled" : {
          "title" : "Port Check Enable",
          "description" : "Indicates if port check functionality is enabled or disabled. (property
 name: org.forgerock.agents.port.check.enabled) ",
          "propertyOrder" : 7200,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "unwantedHttpUrlRegexParams" : {
          "title" : "Regular Expression Remove Query Parameters",
          "description" : "Specifies a list of regular expressions the agent uses to match query
 parameters to be removed from a URL for policy decision and caching purposes. The property has the
```

```
format [Domain/path] | regular_expression[,regular_expression...] with no spaces between values.
(property: org.forgerock.agents.unwanted.http.url.params.regex.list)",
         "propertyOrder" : 19600,
         "required" : false,
         "items" : {
           "type" : "string"
         },
         "type" : "array",
         "exampleValue" : ""
       },
       "localeLanguage" : {
         "title" : "Locale Language",
         "description" : "(property name: org.forgerock.agents.locale.language) <br>Required Agent
Restart",
         "propertyOrder" : 1300,
         "required" : false,
         "type" : "string",
         "exampleValue" : ""
       },
       "authFailReasonUrl" : {
         "title" : "Authentication Fail Reason Url",
         "description" : "This property allows administrators to set the URL/URI of a web page that
says that authentication failed and which may, using the login fail reason parameter, explain why.
(property: org.forgerock.agents.authn.fail.url)",
         "propertyOrder" : 18900,
         "required" : false,
         "type" : "string",
         "exampleValue" : ""
       },
       "loginReasonParameterName" : {
         "title" : "Login Reason Parameter Name",
         "description" : "Property to say why the user is being asked to login, the agent will (in
custom login mode ONLY) pass the named parameter to the custom login endpoint, with an appropriate
value.  Note that this property is not enabled by default as this additional information represents
an information leak. Default reasons: NO_TOKEN, JWT_INVALID, TOKEN_EXPIRED, EXCEPTION. (property:
org.forgerock.agents.login.reason.parameter.name)",
         "propertyOrder" : 18700,
         "required" : false,
         "type" : "string",
         "exampleValue" : ""
       },
       "localeCountry" : {
         "title" : "Locale Country",
         "description" : "(property name: org.forgerock.agents.locale.country) <br>Required Agent
Restart",
         "propertyOrder" : 1400,
         "required" : false,
         "type" : "string",
         "exampleValue" : ""
       },
       "legacyUserAgentList" : {
         "title" : "Legacy User Agent List",
         "description" : "List of user agent header values that identify legacy
browsers. Entries in this list can have wild card character '*'. (property name:
org.forgerock.agents.legacy.user.agent.list) ",
         "propertyOrder" : 6800,
         "required" : false,
         "items" : {
           "type" : "string"
```

```
          },
          "type" : "array",
          "exampleValue" : ""
        }
      }
    },
    "amServicesJ2EEAgent" : {
      "type" : "object",
      "title" : "AM Services",
      "propertyOrder" : 3,
      "properties" : {
        "restrictToRealm" : {
          "title" : "Restrict To Realm",
          "description" : "A map keyed by application name which allows users from only the
 specified realms (each entry is a CSV) to access the specified application. If no restricted
 realm is set, any user from any realm will be allowed access. Keyed by application name,
 value is a comma separated list of realms from which users may request resources. (property:
 org.forgerock.agents.restrict.to.realm.map)",
          "propertyOrder" : 13080,
          "required" : false,
          "patternProperties" : {
            ".*" : {
              "type" : "string"
            }
          },
          "type" : "object",
          "exampleValue" : ""
        },
        "conditionalLogoutUrl" : {
          "title" : "AM Conditional Logout URL",
          "description" : "(property name: org.forgerock.agents.conditional.logout.url.list)
  <br> Examples: <br> match|url?param1=value1&amp;param2=value2 <br> match/path|?
param1=value1&amp;param2=value2&amp;param3=value3",
          "propertyOrder" : 12550,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "policyEvaluationRealm" : {
          "title" : "Policy Evaluation Realm",
          "description" : "Which realm to start evaluating from. (property name:
 org.forgerock.agents.policy.evaluation.realm.map) ",
          "propertyOrder" : 5400,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "urlPolicyEnvPostParameters" : {
          "title" : "URL Policy Env POST Parameters",
          "description" : "List of HTTP POST request parameters whose names and values
 will be set in the environment map for URL policy evaluation at AM server. (property name:
 org.forgerock.agents.continuous.security.post.list)  <br> Examples: <br> name <br> phonenumber",
          "propertyOrder" : 11900,
          "required" : false,
          "items" : {
            "type" : "string"
```

```
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "authServiceHost" : {
          "title" : "AM Authentication Service Host Name",
          "description" : "Host name to be used by the AM authentication service. This property need
 to be updated in OpenSSOAgentBootstrap.properties (property name: org.forgerock.agents.am.hostname)
 <br>Required Agent Restart",
          "propertyOrder" : 11000,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "authServicePort" : {
          "title" : "AM Authentication Service Port",
          "description" : "Port to be used by the AM authentication service. This property need
 to be updated in OpenSSOAgentBootstrap.properties (property name: org.forgerock.agents.am.port)
 <br>Required Agent Restart",
          "propertyOrder" : 11100,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "amLoginUrl" : {
          "title" : "AM Login URL",
          "description" : "AM login page URL. (property name:
 com.sun.identity.agents.config.login.url)  <br> Example: <br> http://host:port/am/UI/Login",
          "propertyOrder" : 3710,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "urlPolicyEnvJsessionParameters" : {
          "title" : "URL Policy Env jsession Parameters",
          "description" : "List of HTTP SESSION attributes whose names and values will
 be set in the environment map for URL policy evaluation at AM server. (property name:
 org.forgerock.agents.continuous.security.http.session.list)  <br> Examples: <br> name <br>
 phonenumber",
          "propertyOrder" : 12000,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "legacyLoginUrlList" : {
          "title" : "Custom Conditional Login URL",
          "description" : "Conditionally redirect users based on the incoming request URL.
 If the incoming request URL matches a specified domain name, the Java agent redirects
 the request to a specific URL. Conditional redirects have the format [Domain/path]|
[URL?realm=value&amp;parameter1=value1...], with no spaces between values. <br>Example:
 myapp.domain.com|https://login.example.com/apps/login.jsp?realm=sales  <br>(property:
 org.forgerock.openam.agents.config.conditional.custom.login.url)",
          "propertyOrder" : 3900,
```

```
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "authServiceProtocol" : {
          "title" : "AM Authentication Service Protocol",
          "description" : "Protocol to be used by the AM authentication service. This property need
 to be updated in OpenSSOAgentBootstrap.properties (property name: org.forgerock.agents.am.protocol)
 <br>Required Agent Restart",
          "propertyOrder" : 10900,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "customLoginEnabled" : {
          "title" : "Allow Custom Login Mode",
          "description" : "Flag to enable custom login. (property:
 org.forgerock.agents.legacy.login.enabled)",
          "propertyOrder" : 3700,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "urlPolicyEnvGetParameters" : {
          "title" : "URL Policy Env GET Parameters",
          "description" : "List of HTTP GET request parameters whose names and values will
 be set in the environment map for URL policy evaluation at AM server. (property name:
 org.forgerock.agents.continuous.security.get.list)  <br> Examples: <br> name <br> phonenumber",
          "propertyOrder" : 11800,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "policyNotifications" : {
          "title" : "Enable Policy Notifications",
          "description" : "Enable Notifications(via websockets) for remote policy client. (property
 name: org.forgerock.agents.policy.change.notifications.enabled) <br>Required Agent Restart",
          "propertyOrder" : 11200,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "conditionalLoginUrl" : {
          "title" : "AM Conditional Login URL",
          "description" : "(property name: org.forgerock.openam.agents.config.conditional.login.url)
  <br> Examples: <br> match|url?param1=value1&amp;ampparam2=value2 <br> match/path|?
param1=value1&amp;ampparam2=value2&amp;ampparam3=value3",
          "propertyOrder" : 3800,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
```

```
          "exampleValue" : ""
        },
        "policyEvaluationApplication" : {
          "title" : "Policy Set",
          "description" : "Which application contains the policies to evaluate with. (property name:
org.forgerock.agents.policy.set.map) ",
          "propertyOrder" : 5500,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "agentAdviceEncode" : {
          "title" : "Composite Advice Encode",
          "description" : "This property is used to specify whether AM composite advices
should be based64url encoded before sending to custom login endpoints. (property:
org.forgerock.agents.advice.b64.url.encode)",
          "propertyOrder" : 13050,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "authSuccessRedirectUrl" : {
          "title" : "Redirect to AM's Success URL",
          "description" : "When enabled, the Agent will redirect to the session's Success URL instead
(defined in auth. chain) of the originally requested resource after successful authentication.
(property: org.forgerock.agents.authn.success.redirect.session.url.enabled)",
          "propertyOrder" : 4000,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        }
      }
    },
    "ssoJ2EEAgentConfig" : {
      "type" : "object",
      "title" : "SSO",
      "propertyOrder" : 2,
      "properties" : {
        "setCookieInternalMap" : {
          "title" : "Set-Cookie Internal Map",
          "description" : "Text from this map will be added directly into the Set-Cookie header
when creating \"internal\" cookies (e.g. the am-auth-jwt and pre-auth cookies). This allows, among
other things, the same-site value to be manipulated. The key is the cookie name, the value is any
arbitrary text suitable for the Set-Cookie header. Users should remember semicolons if they wish
to add multiple values.  Values inappropriate for the header will likely cause the Agent to fail to
create the relevant cookie. (property: org.forgerock.agents.set.cookie.internal.map)",
          "propertyOrder" : 5940,
          "required" : false,
          "patternProperties" : {
            ".*" : {
              "type" : "string"
            }
          },
          "type" : "object",
          "exampleValue" : ""
        },
        "excludedUserAgentsList" : {
          "title" : "Samesite Cookie Attributes Excluded User Agents Pattern List",
```

```
          "description" : "Excluded User agents pattern list. List of incompatible
user agents that will be prevented from receiving SameSite cookie attributes. <br>
(Property:org.forgerock.agents.samesite.excluded.user.agents.list)",
          "propertyOrder" : 5960,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "httpOnly" : {
          "title" : "Http Only",
          "description" : "Flag saying whether HTTP only cookies are enabled. (property:
com.sun.identity.cookie.httponly)",
          "propertyOrder" : 5910,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "cdssoDomainList" : {
          "title" : "CDSSO Domain List",
          "description" : "Domains for which cookies have to be set in a CDSSO scenario. (property
name: org.forgerock.agents.jwt.cookie.domain.list)  <br> Example: <br> .sun.com",
          "propertyOrder" : 5800,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "authExchangeUri" : {
          "title" : "Authentication Exchange URI",
          "description" : "This property allows the administrator to enable an endpoint that will
facilitate the exchange of SSO tokens for OIDC JWTs. The value is empty by default and thus the
endpoint is not accessible. (property: org.forgerock.agents.authn.exchange.uri) (Agent 5.7+ only)",
          "propertyOrder" : 5901,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "setCookieAttributeMap" : {
          "title" : "Set-Cookie Attribute Map",
          "description" : "Text from this map will be added directly into the Set-Cookie header
by the AttributeTaskHandler and its decendents when it creates cookies out of Profile Attributes,
Session Info Attributes and/or Response Attributes. The key is the cookie name, the value is any
arbitrary text suitable for the Set-Cookie header. Users should remember semicolons if they wish
to add multiple values.  Values inappropriate for the header will likely cause the Agent to fail to
create the relevant cookie. (property: org.forgerock.agents.set.cookie.attribute.map)",
          "propertyOrder" : 5950,
          "required" : false,
          "patternProperties" : {
            ".*" : {
              "type" : "string"
            }
          },
          "type" : "object",
          "exampleValue" : ""
```

```
      },
      "acceptIPDPCookie" : {
        "title" : "Convert SSO Tokens into OpenID Connect JWTs",
        "description" : "When this property is set to true, for each incoming request, when the
user does not present a JWT in the designated cookie, the Agent will look for an SSO token in the
iPlanetDirectoryPro cookie (configurable in AM). If this is found, the Agent invokes AM to exchange
it for a JWT which is then used in further requests. The result is cached, so interaction with AM
will not be needed, if the same SSO token is presented in the future (and the existing cache entry is
still valid) (property: org.forgerock.agents.accept.ipdp.cookie.enabled)",
        "propertyOrder" : 5900,
        "required" : false,
        "type" : "boolean",
        "exampleValue" : ""
      },
      "encodeCookies" : {
        "title" : "Encode Cookies",
        "description" : "Cookies are encoded, if set. (property: com.iplanet.am.cookie.encode)",
        "propertyOrder" : 5920,
        "required" : false,
        "type" : "boolean",
        "exampleValue" : ""
      },
      "cookieResetDomains" : {
        "title" : "Cookies Reset Domain Map",
        "description" : "Maps cookie names specified in Cookie Reset Name List to value
being the domain of this cookie to be used when a reset event occurs. (property name:
org.forgerock.agents.cookie.reset.domain.map) ",
        "propertyOrder" : 4800,
        "required" : false,
        "patternProperties" : {
          ".*" : {
            "type" : "string"
          }
        },
        "type" : "object",
        "exampleValue" : ""
      },
      "cdssoSecureCookies" : {
        "title" : "CDSSO Secure Enable",
        "description" : "The SSO Token cookie set by the agent in the different domains in CDSSO
mode will be marked secure. Only transmitted if the communications channel with host is a secure one.
(property name: org.forgerock.agents.secure.cookies.enabled) ",
        "propertyOrder" : 5700,
        "required" : false,
        "type" : "boolean",
        "exampleValue" : ""
      },
      "cdssoRedirectUri" : {
        "title" : "CDSSO Redirect URI",
        "description" : "An intermediate URI that is used by the Agent for processing CDSSO
requests. (property name: org.forgerock.agents.authn.redirect.uri) ",
        "propertyOrder" : 5100,
        "required" : false,
        "type" : "string",
        "exampleValue" : ""
      },
      "cookieResetEnabled" : {
        "title" : "Cookie Reset",
```

```
          "description" : "Agent resets cookies in the response before redirecting to authentication.
(property name: org.forgerock.agents.cookie.reset.enabled) ",
          "propertyOrder" : 4600,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "cookieResetPaths" : {
          "title" : "Cookies Reset Path Map",
          "description" : "Maps cookie names specified in Cookie Reset Name List to value
being the path of this cookie to be used when a reset event occurs. (property name:
org.forgerock.agents.cookie.reset.path.map) ",
          "propertyOrder" : 4900,
          "required" : false,
          "patternProperties" : {
            ".*" : {
              "type" : "string"
            }
          },
          "type" : "object",
          "exampleValue" : ""
        },
        "authExchangeCookieName" : {
          "title" : "Authentication Exchange Cookie Name",
          "description" : "This property allows the administrator to define a cooke name that will be
used by the authn exchange endpoint. The value is empty by default and the endpoint will thus not be
capable of examining cookie values (property: org.forgerock.agents.authn.exchange.cookie.name) (Agent
5.7+ only)",
          "propertyOrder" : 5902,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "cookieResetNames" : {
          "title" : "Cookies Reset Name List",
          "description" : "Cookie names that will be reset by the Agent if Cookie Reset is enabled.
(property name: org.forgerock.agents.cookie.reset.name.list) ",
          "propertyOrder" : 4700,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "secureCookies" : {
          "title" : "Secure Cookies",
          "description" : "On setting this property to true, all cookies created by the
Agent will be secure. The value is set to false for backwards compatibility. (property:
org.forgerock.agents.jwt.cookie.secure.enabled)",
          "propertyOrder" : 5930,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        }
      }
    },
    "advancedJ2EEAgentConfig" : {
      "type" : "object",
```

```
      "title" : "Advanced",
      "propertyOrder" : 5,
      "properties" : {
        "monitoringToCSV" : {
          "title" : "Export Monitoring Metrics to CSV",
          "description" : "When set to true, the Agent will write monitoring information to CSV files.
 (property: org.forgerock.agents.monitoring.to.csv.enabled)",
          "propertyOrder" : 13085,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "customProperties" : {
          "title" : "Custom Properties",
          "description" : "Additional properties that allow users to augment the set of
 properties supported by agent. (property name: com.sun.identity.agents.config.freeformproperties)
  <br> Examples: <br> customproperty=custom-value1 <br> customlist[0]=customlist-value-0
 <br> customlist[1]=customlist-value-1 <br> custommap[key1]=custommap-value-1 <br>
 custommap[key2]=custommap-value-2",
          "propertyOrder" : 20000,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "fragmentRelayUri" : {
          "title" : "Fragment Relay URI",
          "description" : "To enable unauthenticated fragment retention within incoming requests, set
 this property to a valid dummy URI within the Agent application.<br>Example: /agentapp/pre-authn-
fragment-capture <br>(property: org.forgerock.agents.authn.fragment.relay.uri) (Agent 5.7+ only)",
          "propertyOrder" : 13090,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "ssoExchangeCacheTTL" : {
          "title" : "Exchanged SSO Token Cache Time to Live",
          "description" : "This sets the time in minutes after which entries in the SSO token
 exchange cache will timeout and be purged.  Since exchanging SSO tokens for JWTs is an expensive
 process, previously exchanged SSO tokens are cached so that the roundtrip to AM can be avoided
 in the case where an entity is unable to permanently store its JWT in a cookie. (property:
 org.forgerock.agents.sso.exchange.cache.ttl.minutes) <br>Required Agent Restart",
          "propertyOrder" : 13900,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "clientIpHeader" : {
          "title" : "Client IP Address Header",
          "description" : "HTTP header name that holds the IP address of the client. (property name:
 org.forgerock.agents.http.header.containing.ip.address) ",
          "propertyOrder" : 1000,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "missingPostDataPreservationEntryUri" : {
```

```
          "title" : "Missing PDP entry URI",
          "description" : "An application-specific URI Map that is used in case the referenced
PDP entry cannot be found in the local cache (due to ttl). In such cases it will redirect
to the specified URI, otherwise it will show a HTTP 403 Forbidden error. (property name:
org.forgerock.agents.pdp.noentry.url.map)<br>Examples: <br>To set a redirect target for application
BankApp: enter Bankapp in Map Key field and enter a redirect URI in corresponding Map Value field.",
          "propertyOrder" : 13200,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "ssoExchangeCacheSize" : {
          "title" : "Exchanged SSO Token Cache Size",
          "description" : "The number of entries in the SSO Exchange cache. (property:
org.forgerock.agents.sso.exchange.cache.size) <br>Required Agent Restart",
          "propertyOrder" : 13910,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "alternativeAgentHostname" : {
          "title" : "Alternative Agent Host Name",
          "description" : "Host name identifying the Agent protected server to the client browsers if
different from the actual host name. (property name: org.forgerock.agents.agent.hostname) ",
          "propertyOrder" : 4100,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "postDataCacheTtlMin" : {
          "title" : "PDP Cache TTL in Minutes",
          "description" : "This sets the time in minutes after which entries in the Post Data
Preservation cache will timeout and be purged. (property: org.forgerock.agents.pdp.cache.ttl.minutes)
<br>Required Agent Restart",
          "propertyOrder" : 13300,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "idleTimeRefreshWindow" : {
          "title" : "Idle Time Refresh Window",
          "description" : "Once every this number of minutes, the Agent will nudge AM so
it knows a particular session is still in use, thereby resetting its idle time. (property:
org.forgerock.agents.idle.time.window.minutes)",
          "propertyOrder" : 14200,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "postDataStickySessionMode" : {
          "title" : "PDP Stickysession mode",
          "description" : "If the PDP mechanism needs sticky loadbalancing, the URL mode
will append a querystring, while the Cookie mode will create a cookie. (property name:
org.forgerock.agents.pdp.sticky.session.mode)",
          "propertyOrder" : 13400,
          "required" : false,
```

```
          "type" : "string",
          "exampleValue" : ""
        },
        "possibleXssCodeElements" : {
          "title" : "Possible XSS code elements",
          "description" : "If one of these strings occurs in the request, the client is redirected to
an error page. (property name: org.forgerock.agents.xss.code.element.list) ",
          "propertyOrder" : 12800,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "xssDetectionRedirectUri" : {
          "title" : "XSS detection redirect URI",
          "description" : "An application-specific Map that identifies a URI of the customized page if
XSS code has been deteced. (property name: org.forgerock.agents.xss.redirect.uri.map)  <br>Examples:
<br>To set a redirect target for application BankApp: enter BankApp in Map Key field, and enter a
redirect URI in Corresponding Map Value field.",
          "propertyOrder" : 12900,
          "required" : false,
          "patternProperties" : {
            ".*" : {
              "type" : "string"
            }
          },
          "type" : "object",
          "exampleValue" : ""
        },
        "postDataPreserveCacheEntryMaxTotalSizeMb" : {
          "title" : "PDP Maximum Cache Size",
          "description" : "Maximum size of the PDP cache, in megabytes (Property name:
org.forgerock.agents.pdp.cache.total.size.mb).",
          "propertyOrder" : 13600,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "policyClientPollingInterval" : {
          "title" : "Policy Cache TTL",
          "description" : "This sets the time in minutes after which entries in the policy cache will
timeout and be purged. (property name: org.forgerock.agents.policy.cache.ttl.minutes) <br>Required
Agent Restart",
          "propertyOrder" : 13950,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "clientHostnameHeader" : {
          "title" : "Client Hostname Header",
          "description" : "HTTP header name that holds the Hostname of the client. (property name:
org.forgerock.agents.http.header.containing.remote.hostname) ",
          "propertyOrder" : 1100,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
```

```
       "postDataPreserveCacheEntryMaxEntries" : {
         "title" : "PDP Maximum Number of Cache Entries",
         "description" : "Maximum number of entries to hold in the PDP cache (Property name:
org.forgerock.agents.pdp.cache.size).",
         "propertyOrder" : 13550,
         "required" : false,
         "type" : "integer",
         "exampleValue" : ""
       },
       "jwtCacheSize" : {
         "title" : "JWT Cache Size",
         "description" : "The maximum number of entries in the JWT cache. (property:
org.forgerock.agents.jwt.cache.size) <br>Required Agent Restart",
         "propertyOrder" : 13810,
         "required" : false,
         "type" : "integer",
         "exampleValue" : ""
       },
       "policyCacheSize" : {
         "title" : "Policy Cache Size",
         "description" : "The maximum number of sessions, i.e. distinct users, stored in the
policy evaluation cache at any one time. (property: org.forgerock.agents.policy.cache.session.size)
<br>Required Agent Restart",
         "propertyOrder" : 14000,
         "required" : false,
         "type" : "integer",
         "exampleValue" : ""
       },
       "postDataPreservation" : {
         "title" : "Post Data Preservation enabled",
         "description" : "Post Data Preservation functionality basically stores any POST
data before redirecting the user to the login screen and after successful login the agent
will generate a page that autosubmits the same POST to the original URL. (property name:
org.forgerock.agents.post.data.preservation.enabled)",
         "propertyOrder" : 13100,
         "required" : false,
         "type" : "boolean",
         "exampleValue" : ""
       },
       "policyCachePerUser" : {
         "title" : "Policy Cache Per User",
         "description" : "This is the number of distinct policy evaluation entries that each session
(stored in the policy evaluation cache) can have.  Thus the total number of policy evaluation
results that can be stored is the \"Policy Cache Size\" multiplied by the \"Policy Cache Per User\".
(property: org.forgerock.agents.policy.cache.per.session.size) <br>Required Agent Restart",
         "propertyOrder" : 14100,
         "required" : false,
         "type" : "integer",
         "exampleValue" : ""
       },
       "alternativeAgentPort" : {
         "title" : "Alternative Agent Port Number",
         "description" : "Port number identifying the Agent protected server listening
port to the client browsers if different from the actual listening port. (property name:
org.forgerock.agents.agent.port) ",
         "propertyOrder" : 4200,
         "required" : false,
         "type" : "string",
         "exampleValue" : ""
```

```
        },
        "postDataStickySessionKeyValue" : {
          "title" : "PDP Stickysession key-value",
          "description" : "The provided key-value pair will be used for adding to the URL or creating
 the cookie. <br>Example: <br>Set 'lb=server1' to append to the querystring or to have 'lb' cookie
 with 'server1' value. (property name: org.forgerock.agents.pdp.sticky.session.value)",
          "propertyOrder" : 13500,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "alternativeAgentProtocol" : {
          "title" : "Alternative Agent Protocol",
          "description" : "Protocol being used (http/https) by the client browsers to communicate with
 the Agent protected server if different from the actual protocol used by the server. (property name:
 org.forgerock.agents.agent.protocol) ",
          "propertyOrder" : 4300,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sessionCacheTTL" : {
          "title" : "Session Cache TTL",
          "description" : "This sets the time in minutes after which entries in the session cache
 will timeout and be purged.  If an entry is not cached, the Agent will need to retrieve session
 information from AM, hence by default the timeout is much longer than for the policy cache.
 (property: org.forgerock.agents.session.cache.ttl.minutes) <br>Required Agent Restart",
          "propertyOrder" : 13700,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "jwtCacheTTL" : {
          "title" : "JWT Cache TTL",
          "description" : "This sets the time in minutes after which entries in the JWT cache will
 timeout and be purged.  Since all JWTs in the cache have been parsed, and parsing is a CPU intensive
 process, having a large timeout on this cache is advantageous and will save CPU cycles reparsing
 already seen JWTs (property: org.forgerock.agents.jwt.cache.ttl.minutes) <br>Required Agent Restart",
          "propertyOrder" : 13800,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "postDataCacheTtl" : {
          "title" : "PDP Cache TTL in Milliseconds",
          "description" : "This value tells how long a given POST entry should be stored in the
 local cache (in milliseconds), default value is 300000. DEPRECATED: use \"PDP Cache TTL in Minutes
\" instead (property name: com.sun.identity.agents.config.postdata.preserve.cache.entry.ttl)
 <br>Required Agent Restart",
          "propertyOrder" : 13310,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        }
      }
    }
  }
}
```

delete

Usage:

```
am> delete J2EEAgentGroups --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action J2EEAgentGroups --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action J2EEAgentGroups --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action J2EEAgentGroups --realm Realm --actionName nextdescendents
```

query

Querying the agent groups of a specific type

Usage:

```
am> query J2EEAgentGroups --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read J2EEAgentGroups --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update J2EEAgentGroups --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "applicationJ2EEAgentConfig" : {
      "type" : "object",
      "title" : "Application",
      "propertyOrder" : 1,
      "properties" : {
        "notEnforcedFavicon" : {
          "title" : "Not Enforced Favicon",
          "description" : "This flag, if enabled, automatically adds \"*/favicon.ico\" to
 the not enforced list.  This can help to avoid odd situations in which a user is required to
 log in after logging out, just because favicon.ico has been requested by browser. (property:
 org.forgerock.agents.auto.not.enforce.favicon.enabled) <br>Required Agent Restart",
          "propertyOrder" : 7650,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "continuousSecurityHeaders" : {
          "title" : "Continuous Security Headers",
          "description" : "The name of the headers in the user's original request, that will be sent
 as part of the payload during policy evaluation, which can then be accessed via the 'environment'
 variable in a policy script. The 'key' is the name of the header to be sent, and the 'value' is the
 name which it will appear as in the policy evaluation script.It is possible to map multiple headers
 to the same name (they will simply appear as an array in the evaluation script). If the header
 doesn't exist, then the empty string will be sent.",
```

```
          "propertyOrder" : 3211,
          "required" : false,
          "patternProperties" : {
            ".*" : {
              "type" : "string"
            }
          },
          "type" : "object",
          "exampleValue" : ""
        },
        "resourceAccessDeniedUri" : {
          "title" : "Resource Access Denied URI",
          "description" : "An application-specific Map that identifies a URI of the customized access
denied page. (property name: org.forgerock.agents.access.denied.uri.map) <br>Valid key: the web
application name. <br>Valid value: the customized application access denied page URI. <br>For this
property, a global value can be set to apply to all the applications that don't have their own
specific access denied page.  <br> Examples: <br>To set a global access denied page: leave Map Key
field empty, and enter the global access denied page URI /sample/accessdenied.html in Corresponding
Map Value field. <br> To set the access denied page URI for application BankApp: enter BankApp
in Map Key field, and enter the application access denied page URI /BankApp/accessdenied.html in
Corresponding Map Value field.",
          "propertyOrder" : 2700,
          "required" : false,
          "patternProperties" : {
            ".*" : {
              "type" : "string"
            }
          },
          "type" : "object",
          "exampleValue" : ""
        },
        "cookieAttributeUrlEncoded" : {
          "title" : "Attribute Cookie Encode",
          "description" : "Indicates if the value of the attribute should be URL encoded before being
set as a cookie. (property name: org.forgerock.agents.attribute.cookie.encode.enabled) ",
          "propertyOrder" : 8500,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "profileAttributeFetchMode" : {
          "title" : "Profile Attribute Fetch Mode",
          "description" : "The mode of fetching profile attributes. (property name:
com.sun.identity.agents.config.profile.attribute.fetch.mode) ",
          "propertyOrder" : 8700,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "notEnforcedIps" : {
          "title" : "Not Enforced Client IP List",
          "description" : "No authentication and authorization protection from agent
are required for the requests coming from these client IP addresses. (property name:
org.forgerock.agents.notenforced.ip.list)  <br> Examples: <br> 192.18.145.* <br> 192.18.146.123",
          "propertyOrder" : 7900,
          "required" : false,
          "items" : {
            "type" : "string"
          },
```

```
          "type" : "array",
          "exampleValue" : ""
        },
        "cookieAttributeMultiValueSeparator" : {
          "title" : "Cookie Separator Character",
          "description" : "Character that will be used to separate multiple
values of the same attribute when it is being set as a cookie. (property name:
org.forgerock.agents.attribute.cookie.separator) ",
          "propertyOrder" : 8300,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "continuousSecurityCookies" : {
          "title" : "Continuous Security Cookies",
          "description" : "The name of the cookies to be sent as part of the payload during policy
evaluation, which can be accessed via the 'environment' variable in a policy script. The 'key' is
the name of the cookie to be sent, and the 'value' is the name which it will appear as in the policy
evaluation script. It is possible to map multiple cookies to the same name (they will simply appear
as an array in the evaluation script). If the cookie doesn't exist, then the empty string will be
sent.",
          "propertyOrder" : 3210,
          "required" : false,
          "patternProperties" : {
            ".*" : {
              "type" : "string"
            }
          },
          "type" : "object",
          "exampleValue" : ""
        },
        "profileAttributeMap" : {
          "title" : "Profile Attribute Mapping",
          "description" : "Maps the profile attributes to be populated under specific names for the
currently authenticated user. (property name: org.forgerock.agents.profile.attribute.map)  <br>
Example: <br> To populate the value of profile attribute cn under name CUSTOM-Common-Name: enter cn
in Map Key field, and enter CUSTOM-Common-Name in Corresponding Map Value field. <br> To populate
the value of profile attribute mail under name CUSTOM-Email: enter mail in Map Key field, and enter
CUSTOM-Email in Corresponding Map Value field.",
          "propertyOrder" : 8800,
          "required" : false,
          "patternProperties" : {
            ".*" : {
              "type" : "string"
            }
          },
          "type" : "object",
          "exampleValue" : ""
        },
        "notEnforcedIpsCacheSize" : {
          "title" : "Not Enforced IP Cache Size",
          "description" : "Size of the cache to be used if Not Enforced IP Cache Flag is enabled.
(property name: org.forgerock.agents.notenforced.ip.cache.size) ",
          "propertyOrder" : 8200,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "notEnforcedUrisCacheEnabled" : {
```

```
          "title" : "Not Enforced URIs Cache Enabled",
          "description" : "Enables the caching of the Not Enforced URIs list evaluation results.
 (property name: org.forgerock.agents.notenforced.uri.cache.enabled) ",
          "propertyOrder" : 7700,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "notEnforcedUris" : {
          "title" : "Not Enforced URIs",
          "description" : "List of URIs for which protection is not enforced by the Agent. (property
 name: org.forgerock.agents.notenforced.uri.list)  <br> Examples: <br> /BankApp/public/* <br> /
BankApp/images/*",
          "propertyOrder" : 7500,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "logoutIntrospection" : {
          "title" : "Logout Introspect Enabled",
          "description" : "Allows the Agent to search HTTP request body to locate logout parameter.
 (property name: org.forgerock.agents.logout.introspection.enabled) ",
          "propertyOrder" : 6200,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "responseAttributeFetchMode" : {
          "title" : "Response Attribute Fetch Mode",
          "description" : "The mode of fetching policy response attributes. (property name:
 com.sun.identity.agents.config.response.attribute.fetch.mode) ",
          "propertyOrder" : 9100,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "responseAttributeMap" : {
          "title" : "Response Attribute Mapping",
          "description" : "Maps the policy response attributes to be populated under specific names
 for the currently authenticated user. (property name: org.forgerock.agents.response.attribute.map)
 <br> Example: <br> To populate the value of response attribute uid under name CUSTOM-USER-NAME: enter
 uid in Map Key field, and enter CUSTOM-USER-NAME in Corresponding Map Value field.",
          "propertyOrder" : 9200,
          "required" : false,
          "patternProperties" : {
            ".*" : {
              "type" : "string"
            }
          },
          "type" : "object",
          "exampleValue" : ""
        },
        "logoutEntryUri" : {
          "title" : "Logout Entry URI",
          "description" : "An application-specific Map that identifies a URI to be used as an entry
 point after successful logout and subsequent successful authentication if applicable. (property name:
```

```
 org.forgerock.agents.logout.goto.map) <br>Valid key: the web application name. <br>Valid value: the
 logout entry URI. <br>For this property, a global value can be set to apply to all the applications
 that don't have their own specific logout entry URI.   <br> Examples: <br>To set a global application
 logout entry URI: leave Map Key field empty, and enter the global application logout entry URI /
welcome.html in Corresponding Map Value field. <br> To set the logout entry URI for application
 BankApp: enter BankApp in Map Key field, and enter the logout entry URI /BankApp/welcome.html in
 Corresponding Map Value field.",
          "propertyOrder" : 6300,
          "required" : false,
          "patternProperties" : {
            ".*" : {
              "type" : "string"
            }
          },
          "type" : "object",
          "exampleValue" : ""
        },
        "sessionAttributeFetchMode" : {
          "title" : "Session Attribute Fetch Mode",
          "description" : "The mode of fetching session attributes. (property name:
 com.sun.identity.agents.config.session.attribute.fetch.mode) ",
          "propertyOrder" : 8900,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "applicationLogoutUris" : {
          "title" : "Application Logout URI",
          "description" : "An application-specific Map that identifies a request URI which indicates
 a logout event. (property name: org.forgerock.agents.logout.endpoint.map) <br>Valid key: the web
 application name. <br>Valid value: the application logout URI. <br>For this property, a global value
 can be set to apply to all the applications that don't have their own specific logout URI.  <br>
 Examples: <br>To set a global application logout URI: leave Map Key field empty, and enter the global
 application logout URI /logout.jsp in Corresponding Map Value field. <br> To set the logout URI for
 application BankApp: enter BankApp in Map Key field, and enter the application logout URI /BankApp/
logout.jsp in Corresponding Map Value field.",
          "propertyOrder" : 6000,
          "required" : false,
          "patternProperties" : {
            ".*" : {
              "type" : "string"
            }
          },
          "type" : "object",
          "exampleValue" : ""
        },
        "notEnforcedIpsCacheEnabled" : {
          "title" : "Not Enforced IP Cache Flag",
          "description" : "Enable caching of not-enforced IP list evaluation results. (property name:
 org.forgerock.agents.notenforced.ip.cache.enabled) ",
          "propertyOrder" : 8100,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "headerAttributeDateFormat" : {
          "title" : "Fetch Attribute Date Format",
```

```
          "description" : "Format of date attribute values to be used when the attribute is
 being set as HTTP header. Format is based on java.text.SimpleDateFormat. (property name:
 org.forgerock.agents.attribute.date.format) ",
          "propertyOrder" : 8400,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "notEnforcedUrisCacheSize" : {
          "title" : "Not Enforced URIs Cache Size",
          "description" : "Size of the cache to be used if caching of not enforced URI list evaluation
 results is enabled. (property name: org.forgerock.agents.notenforced.uri.cache.size) ",
          "propertyOrder" : 7800,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "sessionAttributeMap" : {
          "title" : "Session Attribute Mapping",
          "description" : "Maps the session attributes to be populated under specific names for the
 currently authenticated user. (property name: org.forgerock.agents.session.attribute.map)   <br>
 Example: <br>  To populate the value of session attribute UserToken under name CUSTOM-userid: enter
 UserToken in Map Key field, and enter CUSTOM-userid in Corresponding Map Value field.",
          "propertyOrder" : 9000,
          "required" : false,
          "patternProperties" : {
            ".*" : {
              "type" : "string"
            }
          },
          "type" : "object",
          "exampleValue" : ""
        },
        "logoutRequestParameters" : {
          "title" : "Logout Request Parameter",
          "description" : "An application-specific Map that identifies a parameter
 which when present in the HTTP request indicates a logout event. (property name:
 org.forgerock.agents.logout.request.param.map)  <br>Valid key: the web application name. <br>Valid
 value: the logout request parameter. <br>For this property, a global value can be set to apply to
 all the applications that don't have their own specific logout request parameter.   <br> Examples:
 <br>To set a global application logout request parameter: leave Map Key field empty, and enter the
 global application logout request parameter logoutparam in Corresponding Map Value field. <br> To set
 the logout request parameter for application BankApp: enter BankApp in Map Key field, and enter the
 logout request parameter logoutparam in Corresponding Map Value field.",
          "propertyOrder" : 6100,
          "required" : false,
          "patternProperties" : {
            ".*" : {
              "type" : "string"
            }
          },
          "type" : "object",
          "exampleValue" : ""
        },
        "loginFormUri" : {
          "title" : "Login Form URI",
          "description" : "List of absolute URIs corresponding to an application's web.xml form-login-
page element. (property name: com.sun.identity.agents.config.login.form)  <br> Example: <br> /BankApp/
jsp/login.jsp",
```

```
          "propertyOrder" : 2800,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "invertNotEnforcedIps" : {
          "title" : "Invert Not Enforced IPs",
          "description" : "Client IP Addresses to invert protection of IP
addresses listed in the related Not Enforced Client IP List. (property name:
org.forgerock.agents.notenforced.ip.invert.enabled) ",
          "propertyOrder" : 8000,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "invertNotEnforcedUris" : {
          "title" : "Invert Not Enforced URIs",
          "description" : "Inverts protection of  URIs specified in Not Enforced URIs list. When set
to true, it indicates that the URIs specified should be enforced and all other URIs should be not
enforced by the Agent. (property name: org.forgerock.agents.notenforced.uri.invert.enabled) ",
          "propertyOrder" : 7600,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "notEnforcedRuleCompoundSeparator" : {
          "title" : "Not Enforced Compound Rule Separator",
          "description" : "Specifies a separator for not enforced compound rules. The format for
compound rules requires a list of IP rules, a separator (by default the | character), and a list of
URI rules. <br>Example, GET 192.168.1.1-192.168.4.3 | /images/* <br>Configure a different separator
(for example, &&) when working with the REGEX keyword to avoid invalid regular expressions.",
          "propertyOrder" : 7450,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "globalJ2EEAgentConfig" : {
      "type" : "object",
      "title" : "Global",
      "propertyOrder" : 0,
      "properties" : {
        "localAuditRotationSize" : {
          "title" : "Local Audit Log Rotation Size",
          "description" : "Size limit when a local audit log file is rotated to a new file. (property
name: com.sun.identity.agents.config.local.log.size) ",
          "propertyOrder" : 1900,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "debugLogfileSuffix" : {
          "title" : "Debug File Rotation Suffix",
          "description" : "This is a value appended onto the end of the debug file name when it is
rotated. The user is free to define it as they want, but if it does not involve a timestamp that
```

```
produces different file names when the rotation time is reached, log file rotation is unlikely to
function correctly (property: org.forgerock.agents.debug.suffix)",
         "propertyOrder" : 10020,
         "required" : false,
         "type" : "string",
         "exampleValue" : ""
       },
       "cdssoRootUrl" : {
         "title" : "Agent Root URL for CDSSO",
         "description" : "The agent root URL for CDSSO. The valid value is in the following format:
<br>protocol://hostname:port/<br> The protocol represents the protocol used, such as http or https.
The hostname represents the host name of the machine on which the agent resides. The port represents
the port number on which the agent is installed. The slash following the port number is required.",
         "propertyOrder" : 22700,
         "required" : false,
         "items" : {
           "type" : "string"
         },
         "type" : "array",
         "exampleValue" : ""
       },
       "localAuditLogfilePath" : {
         "title" : "Audit Logfile Path",
         "description" : "The full path of the local auditing file. (property:
org.forgerock.agents.local.audit.file.path)",
         "propertyOrder" : 2000,
         "required" : false,
         "type" : "string",
         "exampleValue" : ""
       },
       "localAuditLogRotation" : {
         "title" : "Rotate Local Audit Log",
         "description" : "Flag to indicate that audit log files should be rotated when reaching a
certain size. (property name: org.forgerock.agents.local.audit.log.rotation.enabled) ",
         "propertyOrder" : 1800,
         "required" : false,
         "type" : "boolean",
         "exampleValue" : ""
       },
       "debugLogfileDirectory" : {
         "title" : "Debug Logfile Directory",
         "description" : "Location of the agent logs files, and where monitoring CSV files are
written. This is normally set in bootstrap properties during the install process. Note there is no
default and no logging will occur until a value for this property is provided. Anything logged will
be written to the standard output and may end up in the container log file (so \"catalina.out\" in
the case of Tomcat). (property: org.forgerock.agents.csv.monitoring.directory)",
         "propertyOrder" : 10060,
         "required" : false,
         "type" : "string",
         "exampleValue" : ""
       },
       "configurationReloadInterval" : {
         "title" : "Configuration Reload Interval",
         "description" : "Only used when websocket notifications are disabled, specifies
interval in seconds after which config is reloaded automatically by the Agent. (property name:
org.forgerock.agents.config.reload.seconds) ",
         "propertyOrder" : 1200,
         "required" : false,
         "type" : "integer",
```

```
        "exampleValue" : ""
      },
      "loginAttemptLimitCookieName" : {
        "title" : "Login Attempt Limit Cookie Name",
        "description" : "The name of the cookie used to record the number of login attempts.
(property: org.forgerock.agents.login.counter.cookie.name)",
        "propertyOrder" : 4500,
        "required" : false,
        "type" : "string",
        "exampleValue" : ""
      },
      "fallforwardModeEnabled" : {
        "title" : "Fall-Forward Mode",
        "description" : "This property is used when AM is not available. <br>  Disabled: the
Agent will deny every incoming request with an HTTP 403 <br>  Enabled: the Agent will continue
to allow access to any resource matched by a not enforced rule until AM becomes available again
<br><br>(property: org.forgerock.agents.session.change.notifications.enabled) (Agent 5.7+ only)",
        "propertyOrder" : 12115,
        "required" : false,
        "type" : "boolean",
        "exampleValue" : ""
      },
      "debugLogfileRotationMinutes" : {
        "title" : "Debug File Rotation Time",
        "description" : "This is the time in minutes after which log file rotation will occur.
(property: org.forgerock.agents.debug.rotation.time.minutes)",
        "propertyOrder" : 10040,
        "required" : false,
        "type" : "integer",
        "exampleValue" : ""
      },
      "auditLogLocation" : {
        "title" : "Audit Log Location",
        "description" : "LOCAL = audit information stored in files based locally
to the Agent container <br>REMOTE = audit information logged via AM. (property name:
org.forgerock.agents.audit.where) ",
        "propertyOrder" : 1600,
        "required" : false,
        "type" : "string",
        "exampleValue" : ""
      },
      "loginAttemptLimit" : {
        "title" : "Login Attempt Limit",
        "description" : "Limit of failed login attempts for a user's single browser session until
triggering the blocking of the user request. Value of 0 disables this feature. (property name:
org.forgerock.agents.login.attempt.limit.count) ",
        "propertyOrder" : 4400,
        "required" : false,
        "type" : "integer",
        "exampleValue" : ""
      },
      "debugLogfilePrefix" : {
        "title" : "Debug File Rotation Prefix",
        "description" : "Prefix which can be added onto the front of the debug file name when it is
rotated. (property: org.forgerock.agents.debug.prefix)",
        "propertyOrder" : 10010,
        "required" : false,
        "type" : "string",
        "exampleValue" : ""
```

```
      },
      "debugLogfileRetentionCount" : {
        "title" : "Debug File Rotation Retention Count",
        "description" : "This is the number of log files to retain after rotation, so for example,
setting it to 10 would give you one current debug file and nine older (rotated) files. (property:
org.forgerock.agents.debug.retention.count)",
        "propertyOrder" : 10050,
        "required" : false,
        "type" : "integer",
        "exampleValue" : ""
      },
      "redirectAttemptLimit" : {
        "title" : "Redirect Attempt Limit",
        "description" : "Number of successive single point redirects that a user can make using a
single browser session which will trigger the blocking of the user request. Set to 0 to disable this
feature. (property name: org.forgerock.agents.redirect.attempt.limit) ",
        "propertyOrder" : 7100,
        "required" : false,
        "type" : "integer",
        "exampleValue" : ""
      },
      "redirectAttemptLimitCookieName" : {
        "title" : "Redirect Attempt Cookie Name",
        "description" : "Agent tries to detect redirect loops while authenticating, which would
normally indicate a cookie domain problem.  The Agent does this by using a cookie to holds the
current redirection count. (property: org.forgerock.agents.redirect.cookie.name)",
        "propertyOrder" : 7150,
        "required" : false,
        "type" : "string",
        "exampleValue" : ""
      },
      "customResponseHeader" : {
        "title" : "Custom Response Header",
        "description" : "Map specifies the custom headers that are set by the Agent on the client
browser. The key is the header name and the value represents the header value. (property name:
org.forgerock.agents.response.header.map)  <br> Example: <br>  To set the custom header Cache-Control
to value no-cache: enter Cache-Control in Map Key field, and enter no-cache in Corresponding Map
Value field.",
        "propertyOrder" : 7000,
        "required" : false,
        "patternProperties" : {
          ".*" : {
            "type" : "string"
          }
        },
        "type" : "object",
        "exampleValue" : ""
      },
      "filterMode" : {
        "title" : "Agent Filter Mode",
        "description" : "Specifies the mode of operation of the Filter. (property name:
org.forgerock.agents.filter.mode.map) <br>Valid key: the web application name. <br>Valid values:
ALL, URL_POLICY, SSO_ONLY, NONE <br>For this property, a global value can be set to apply to all
the applications that don't have their own specific filter mode. <br>Examples: <br>To set ALL as the
global filter mode: leave Map Key field empty, and enter ALL in Corresponding Map Value field. <br>To
set URL_POLICY as the filter mode for application BankApp: enter BankApp in Map Key field, and enter
URL_POLICY in Corresponding Map Value field.",
        "propertyOrder" : 500,
        "required" : false,
```

```
          "patternProperties" : {
            ".*" : {
              "type" : "string"
            }
          },
          "type" : "object",
          "exampleValue" : ""
        },
        "userPrincipalFlag" : {
          "title" : "User Principal Flag",
          "description" : "Use principal instead of just the user-ID for authenticating the user.
(property name: org.forgerock.agents.userid.mapping.mode.use.dn.enabled) ",
          "propertyOrder" : 800,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "userTokenName" : {
          "title" : "User Token Name",
          "description" : "Session property name for user-ID of the authenticated user in session.
(property name: org.forgerock.agents.userid.mapping.mode.use.session.property.name) ",
          "propertyOrder" : 900,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "fqdnCheck" : {
          "title" : "FQDN Check",
          "description" : "Enables checking of fqdn default value and fqdn map values. (property name:
org.forgerock.agents.fqdn.check.enabled) ",
          "propertyOrder" : 6400,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "preAuthCookieName" : {
          "title" : "Pre-Authenticated Cookie Name",
          "description" : "Specifies the name of the cookie the agent uses to track the progress of
authentication with AM. (property: org.forgerock.agents.authn.cookie.name)",
          "propertyOrder" : 11210,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "preAuthCookieMaxAge" : {
          "title" : "Pre-Authenticated Cookie Max Age",
          "description" : "This is the amount of time in seconds before the pre-authn cookie will
timeout. (property: org.forgerock.agents.authn.cookie.max.age.seconds)",
          "propertyOrder" : 11220,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "agentSessionChangeNotificationsEnabled" : {
          "title" : "Session Logout Notification ",
          "description" : "Flag to indicate whether the Agent will subscribe
to session logout notifications (via websockets) from AM. (property:
org.forgerock.agents.session.change.notifications.enabled)",
          "propertyOrder" : 12110,
```

```
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "userAttributeName" : {
          "title" : "User Attribute Name",
          "description" : "Name of the attribute which contains the user-ID. (property name:
org.forgerock.agents.user.mapping.mode.attribute.name) ",
          "propertyOrder" : 700,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "auditAccessType" : {
          "title" : "Audit Access Types",
          "description" : "Types of messages to log based on user URL access attempts. (property name:
org.forgerock.agents.audit.what) ",
          "propertyOrder" : 1500,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "debugLogfileRotationSize" : {
          "title" : "Debug File Rotation Size",
          "description" : "This specifies the approximate size in bytes at which a log file will be
rotated to a new log file. (property: org.forgerock.agents.debug.rotation.size.bytes)",
          "propertyOrder" : 10030,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "localAuditLogfileRetentionCount" : {
          "title" : "Audit Logfile Retention Count",
          "description" : "The number of audit log files to retain after rotation has occurred.
(property: org.forgerock.agents.local.audit.log.retention.count)",
          "propertyOrder" : 2100,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "httpSessionBinding" : {
          "title" : "HTTP Session Binding",
          "description" : "If true will invalidate the http session when login has failed,
user has no SSO session, or principal user name does not match SSO user name. (property name:
org.forgerock.agents.http.session.binding.enabled) ",
          "propertyOrder" : 3500,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "fqdnMapping" : {
          "title" : "FQDN Virtual Host Map",
          "description" : "Maps virtual, invalid, or partial hostnames, and IP addresses to the
FQDN to access protected resources. (property name: org.forgerock.agents.fqdn.map)  <br> Examples:
<br>  To map the partial hostname myserver to myserver.mydomain.com: enter myserver in the Map
Key field and myserver.mydomain.com in the Corresponding Map Value field. To map a virtual server
rst.hostname.com that points to the actual server abc.hostname.com: enter valid1 in the Map Key field
and rst.hostname.com in the Corresponding Map Value field.",
          "propertyOrder" : 6600,
```

```
          "required" : false,
          "patternProperties" : {
            ".*" : {
              "type" : "string"
            }
          },
          "type" : "object",
          "exampleValue" : ""
        },
        "jwtName" : {
          "title" : "JWT Cookie Name",
          "description" : "The name used by the agent to set the OIDC JWT on the user's browser.
(property: org.forgerock.agents.jwt.cookie.name)",
          "propertyOrder" : 11201,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "agentConfigChangeNotificationsEnabled" : {
          "title" : "Agent Configuration Change Notification",
          "description" : "Enable agent to receive notification messages
(via websockets) from AM server for configuration changes. (property name:
org.forgerock.agents.config.change.notifications.enabled) ",
          "propertyOrder" : 12100,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "debugLevel" : {
          "title" : "Agent Debug Level",
          "description" : "Specifies type of agent debug messages to log. (property name:
com.iplanet.services.debug.level) ",
          "propertyOrder" : 10000,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "status" : {
          "title" : "Status",
          "description" : "Status of the agent configuration.",
          "propertyOrder" : 200,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "webSocketConnectionIntervalInMinutes" : {
          "title" : "Web Socket Connection Interval",
          "description" : "Interval in minutes by which agents reopen their web socket
connection to ensure a fair distribution of connections across AM servers. (property:
org.forgerock.agents.balance.websocket.interval.minutes).",
          "propertyOrder" : 12120,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "userMappingMode" : {
          "title" : "User Mapping Mode",
          "description" : "Specifies mechanism agent uses to determine user-ID. (property name:
org.forgerock.agents.user.mapping.mode) ",
```

```
          "propertyOrder" : 600,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "fqdnDefault" : {
          "title" : "FQDN Default",
          "description" : "Fully qualified hostname that the users should use in order to access
 resources. (property name: org.forgerock.agents.fqdn.default) ",
          "propertyOrder" : 6500,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "miscJ2EEAgentConfig" : {
      "type" : "object",
      "title" : "Miscellaneous",
      "propertyOrder" : 4,
      "properties" : {
        "portCheckFile" : {
          "title" : "Port Check File",
          "description" : "Name or complete path of a file that has the necessary content needed to
 handle requests that need port correction. (property name: org.forgerock.agents.port.check.file) ",
          "propertyOrder" : 7300,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "loginReasonMap" : {
          "title" : "Login Reason Value Map",
          "description" : "This map allows some of the possible reasons to be mapped to
 arbitrary values, when empty will be used default values(see: \"Login Reason Parameter Name
\" description). LOGIN REASON=CUSTOM VALUE e.g. [JWT_INVALID]=corrupted_token. (property:
 org.forgerock.agents.login.reason.remapper)",
          "propertyOrder" : 18800,
          "required" : false,
          "patternProperties" : {
            ".*" : {
              "type" : "string"
            }
          },
          "type" : "object",
          "exampleValue" : ""
        },
        "ignorePathInfo" : {
          "title" : "Ignore Path Info in Request URL",
          "description" : "The path info will be stripped from the request URL while doing Not
 Enforced List check and url policy evaluation if the value is set to true. (property name:
 com.sun.identity.agents.config.ignore.path.info)",
          "propertyOrder" : 18600,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "legacyRedirectUri" : {
          "title" : "Legacy User Agent Redirect URI",
```

```
          "description" : "An intermediate URI used by the Agent to redirect legacy user agent
requests. (property name: org.forgerock.agents.legacy.redirect.uri) ",
          "propertyOrder" : 6900,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "authFailReasonParameterName" : {
          "title" : "Authentication Fail Reason Parameter Name",
          "description" : "If this property is defined, the agent will pass the named parameter
to a custom page (defined by \"Authentication Fail Reason Url\") saying why authentication
failed.  The reason can be very detailed and users may want to use the \"Authentication
Fail Reason Parameter Value Map\" to give custom detail, otherwise these default values
will be used: AUTHN_BOOKKEEPING_COOKIE_MISSING, NONCE_MISSING, EXCEPTION (property:
org.forgerock.agents.authn.fail.reason.parameter.name)",
          "propertyOrder" : 19000,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "wantedHttpUrlRegexParams" : {
          "title" : "Regular Expression Retain Query Parameters",
          "description" : "Specifies a list of regular expressions the agent uses to match query
parameters to be retained for policy decision and caching purposes. The property has the format
[Domain/path] | regular_expression[,regular_expression...] with no spaces between values. (property:
org.forgerock.agents.wanted.http.url.params.regex.list)",
          "propertyOrder" : 19400,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "gotoParameterName" : {
          "title" : "Goto Parameter Name",
          "description" : "This is the name of the HTTP query \"goto\" parameter. It is not
recommended to change it. (property name: com.sun.identity.agents.config.redirect.param) ",
          "propertyOrder" : 3600,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "gotoUrl" : {
          "title" : "Goto Url",
          "description" : "This is a URL used in rare circumstances where the Agent has nowhere
else to go.  For instance if the user requests a resource, authenticates for the first time,
then presses the back button and the administrator hasn't set up the authn fail URL. (property:
org.forgerock.agents.default.goto.url)",
          "propertyOrder" : 19200,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "unwantedHttpUrlParams" : {
          "title" : "Remove Query Parameters",
          "description" : "Specifies a list of query parameters to be removed from a URL for policy
decision and caching purposes. The property has the format [Domain/path] | parameter[,parameter...]
```

```
with no spaces between values (property: org.forgerock.agents.unwanted.http.url.param.list)
<br>Example: myapp.example.com/customers|location,lang",
         "propertyOrder" : 19500,
         "required" : false,
         "items" : {
           "type" : "string"
         },
         "type" : "array",
         "exampleValue" : ""
       },
       "serviceResolverClass" : {
         "title" : "Service Resolver Class Name",
         "description" : "Name of the service resolver class to change in order
to instantiate own service resolver and overriding default ones <br>(property:
org.forgerock.agents.service.resolver.class.name) (Agent 5.6.2+ only) <br> Agent restart is
required",
         "propertyOrder" : 19700,
         "required" : false,
         "type" : "string",
         "exampleValue" : ""
       },
       "authFailReasonParameterRemapper" : {
         "title" : "Authentication Fail Reason Parameter Value Map",
         "description" : "This map allows some of the possible reasons to be
mapped to arbitrary values. When empty, will use default values. (property:
org.forgerock.agents.authn.fail.reason.remapper)",
         "propertyOrder" : 19100,
         "required" : false,
         "patternProperties" : {
           ".*" : {
             "type" : "string"
           }
         },
         "type" : "object",
         "exampleValue" : ""
       },
       "legacyUserAgentSupport" : {
         "title" : "Legacy User Agent Support Enable",
         "description" : "Enables support for legacy user agents (browser). (property name:
org.forgerock.agents.legacy.support.enabled) ",
         "propertyOrder" : 6700,
         "required" : false,
         "type" : "boolean",
         "exampleValue" : ""
       },
       "portCheckSetting" : {
         "title" : "Port Check Setting",
         "description" : "Map of port versus protocol entries with the key being the listening port
number and value being the listening protocol to be used by the Agent to identify requests with
invalid port numbers. (property name: org.forgerock.agents.port.check.map)  <br> Example: <br> To
map port 80 to protocol http: enter 80 in Map Key field, and enter http in Corresponding Map Value
field.",
         "propertyOrder" : 7400,
         "required" : false,
         "patternProperties" : {
           ".*" : {
             "type" : "string"
           }
         },
```

```
          "type" : "object",
          "exampleValue" : ""
        },
        "wantedHttpUrlParams" : {
          "title" : "Retain Query Parameters",
          "description" : "Specifies a list of query parameters to be retained (other parameters
 will be removed) from a URL for policy decision and caching purposes. The property has the
 format [Domain/path] | parameter[,parameter...] with no spaces between values. (property:
 org.forgerock.agents.wanted.http.url.param.list) <br>Example: myapp.example.com/customers|
location,lang",
          "propertyOrder" : 19300,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "portCheckEnabled" : {
          "title" : "Port Check Enable",
          "description" : "Indicates if port check functionality is enabled or disabled. (property
 name: org.forgerock.agents.port.check.enabled) ",
          "propertyOrder" : 7200,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "unwantedHttpUrlRegexParams" : {
          "title" : "Regular Expression Remove Query Parameters",
          "description" : "Specifies a list of regular expressions the agent uses to match query
 parameters to be removed from a URL for policy decision and caching purposes. The property has the
 format [Domain/path] | regular_expression[,regular_expression...] with no spaces between values.
 (property: org.forgerock.agents.unwanted.http.url.params.regex.list)",
          "propertyOrder" : 19600,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "localeLanguage" : {
          "title" : "Locale Language",
          "description" : "(property name: org.forgerock.agents.locale.language) <br>Required Agent
 Restart",
          "propertyOrder" : 1300,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "authFailReasonUrl" : {
          "title" : "Authentication Fail Reason Url",
          "description" : "This property allows administrators to set the URL/URI of a web page that
 says that authentication failed and which may, using the login fail reason parameter, explain why.
 (property: org.forgerock.agents.authn.fail.url)",
          "propertyOrder" : 18900,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
```

```
       },
       "loginReasonParameterName" : {
         "title" : "Login Reason Parameter Name",
         "description" : "Property to say why the user is being asked to login, the agent will (in
custom login mode ONLY) pass the named parameter to the custom login endpoint, with an appropriate
value.  Note that this property is not enabled by default as this additional information represents
an information leak. Default reasons: NO_TOKEN, JWT_INVALID, TOKEN_EXPIRED, EXCEPTION. (property:
org.forgerock.agents.login.reason.parameter.name)",
         "propertyOrder" : 18700,
         "required" : false,
         "type" : "string",
         "exampleValue" : ""
       },
       "localeCountry" : {
         "title" : "Locale Country",
         "description" : "(property name: org.forgerock.agents.locale.country) <br>Required Agent
Restart",
         "propertyOrder" : 1400,
         "required" : false,
         "type" : "string",
         "exampleValue" : ""
       },
       "legacyUserAgentList" : {
         "title" : "Legacy User Agent List",
         "description" : "List of user agent header values that identify legacy
browsers. Entries in this list can have wild card character '*'. (property name:
org.forgerock.agents.legacy.user.agent.list) ",
         "propertyOrder" : 6800,
         "required" : false,
         "items" : {
           "type" : "string"
         },
         "type" : "array",
         "exampleValue" : ""
       }
     }
   },
   "amServicesJ2EEAgent" : {
     "type" : "object",
     "title" : "AM Services",
     "propertyOrder" : 3,
     "properties" : {
       "restrictToRealm" : {
         "title" : "Restrict To Realm",
         "description" : "A map keyed by application name which allows users from only the
specified realms (each entry is a CSV) to access the specified application. If no restricted
realm is set, any user from any realm will be allowed access. Keyed by application name,
value is a comma separated list of realms from which users may request resources. (property:
org.forgerock.agents.restrict.to.realm.map)",
         "propertyOrder" : 13080,
         "required" : false,
         "patternProperties" : {
           ".*" : {
             "type" : "string"
           }
         },
         "type" : "object",
         "exampleValue" : ""
       },
```

```
        "conditionalLogoutUrl" : {
          "title" : "AM Conditional Logout URL",
          "description" : "(property name: org.forgerock.agents.conditional.logout.url.list)
  <br> Examples: <br> match|url?param1=value1&amp;param2=value2 <br> match/path|?
param1=value1&amp;param2=value2&amp;param3=value3",
          "propertyOrder" : 12550,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "policyEvaluationRealm" : {
          "title" : "Policy Evaluation Realm",
          "description" : "Which realm to start evaluating from. (property name:
 org.forgerock.agents.policy.evaluation.realm.map) ",
          "propertyOrder" : 5400,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "urlPolicyEnvPostParameters" : {
          "title" : "URL Policy Env POST Parameters",
          "description" : "List of HTTP POST request parameters whose names and values
 will be set in the environment map for URL policy evaluation at AM server. (property name:
 org.forgerock.agents.continuous.security.post.list)  <br> Examples: <br> name <br> phonenumber",
          "propertyOrder" : 11900,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "authServiceHost" : {
          "title" : "AM Authentication Service Host Name",
          "description" : "Host name to be used by the AM authentication service. This property need
 to be updated in OpenSSOAgentBootstrap.properties (property name: org.forgerock.agents.am.hostname)
 <br>Required Agent Restart",
          "propertyOrder" : 11000,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "authServicePort" : {
          "title" : "AM Authentication Service Port",
          "description" : "Port to be used by the AM authentication service. This property need
 to be updated in OpenSSOAgentBootstrap.properties (property name: org.forgerock.agents.am.port)
 <br>Required Agent Restart",
          "propertyOrder" : 11100,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "amLoginUrl" : {
          "title" : "AM Login URL",
          "description" : "AM login page URL. (property name:
 com.sun.identity.agents.config.login.url)  <br> Example: <br> http://host:port/am/UI/Login",
```

```
          "propertyOrder" : 3710,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "urlPolicyEnvJsessionParameters" : {
          "title" : "URL Policy Env jsession Parameters",
          "description" : "List of HTTP SESSION attributes whose names and values will
 be set in the environment map for URL policy evaluation at AM server. (property name:
 org.forgerock.agents.continuous.security.http.session.list)  <br> Examples: <br> name <br>
 phonenumber",
          "propertyOrder" : 12000,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "legacyLoginUrlList" : {
          "title" : "Custom Conditional Login URL",
          "description" : "Conditionally redirect users based on the incoming request URL.
 If the incoming request URL matches a specified domain name, the Java agent redirects
 the request to a specific URL. Conditional redirects have the format [Domain/path]|
[URL?realm=value&amp;parameter1=value1...], with no spaces between values. <br>Example:
 myapp.domain.com|https://login.example.com/apps/login.jsp?realm=sales  <br>(property:
 org.forgerock.openam.agents.config.conditional.custom.login.url)",
          "propertyOrder" : 3900,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "authServiceProtocol" : {
          "title" : "AM Authentication Service Protocol",
          "description" : "Protocol to be used by the AM authentication service. This property need
 to be updated in OpenSSOAgentBootstrap.properties (property name: org.forgerock.agents.am.protocol)
 <br>Required Agent Restart",
          "propertyOrder" : 10900,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "customLoginEnabled" : {
          "title" : "Allow Custom Login Mode",
          "description" : "Flag to enable custom login. (property:
 org.forgerock.agents.legacy.login.enabled)",
          "propertyOrder" : 3700,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "urlPolicyEnvGetParameters" : {
          "title" : "URL Policy Env GET Parameters",
```

```
          "description" : "List of HTTP GET request parameters whose names and values will
 be set in the environment map for URL policy evaluation at AM server. (property name:
 org.forgerock.agents.continuous.security.get.list)  <br> Examples: <br> name <br> phonenumber",
          "propertyOrder" : 11800,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "policyNotifications" : {
          "title" : "Enable Policy Notifications",
          "description" : "Enable Notifications(via websockets) for remote policy client. (property
 name: org.forgerock.agents.policy.change.notifications.enabled) <br>Required Agent Restart",
          "propertyOrder" : 11200,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "conditionalLoginUrl" : {
          "title" : "AM Conditional Login URL",
          "description" : "(property name: org.forgerock.openam.agents.config.conditional.login.url)
  <br> Examples: <br> match|url?param1=value1&amp;ampparam2=value2 <br> match/path|?
param1=value1&amp;ampparam2=value2&amp;ampparam3=value3",
          "propertyOrder" : 3800,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "policyEvaluationApplication" : {
          "title" : "Policy Set",
          "description" : "Which application contains the policies to evaluate with. (property name:
 org.forgerock.agents.policy.set.map) ",
          "propertyOrder" : 5500,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "agentAdviceEncode" : {
          "title" : "Composite Advice Encode",
          "description" : "This property is used to specify whether AM composite advices
 should be based64url encoded before sending to custom login endpoints. (property:
 org.forgerock.agents.advice.b64.url.encode)",
          "propertyOrder" : 13050,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "authSuccessRedirectUrl" : {
          "title" : "Redirect to AM's Success URL",
          "description" : "When enabled, the Agent will redirect to the session's Success URL instead
 (defined in auth. chain) of the originally requested resource after successful authentication.
 (property: org.forgerock.agents.authn.success.redirect.session.url.enabled)",
          "propertyOrder" : 4000,
          "required" : false,
```

```
          "type" : "boolean",
          "exampleValue" : ""
        }
      }
    },
    "ssoJ2EEAgentConfig" : {
      "type" : "object",
      "title" : "SSO",
      "propertyOrder" : 2,
      "properties" : {
        "setCookieInternalMap" : {
          "title" : "Set-Cookie Internal Map",
          "description" : "Text from this map will be added directly into the Set-Cookie header
when creating \"internal\" cookies (e.g. the am-auth-jwt and pre-auth cookies). This allows, among
other things, the same-site value to be manipulated. The key is the cookie name, the value is any
arbitrary text suitable for the Set-Cookie header. Users should remember semicolons if they wish
to add multiple values.  Values inappropriate for the header will likely cause the Agent to fail to
create the relevant cookie. (property: org.forgerock.agents.set.cookie.internal.map)",
          "propertyOrder" : 5940,
          "required" : false,
          "patternProperties" : {
            ".*" : {
              "type" : "string"
            }
          },
          "type" : "object",
          "exampleValue" : ""
        },
        "excludedUserAgentsList" : {
          "title" : "Samesite Cookie Attributes Excluded User Agents Pattern List",
          "description" : "Excluded User agents pattern list. List of incompatible
user agents that will be prevented from receiving SameSite cookie attributes. <br>
(Property:org.forgerock.agents.samesite.excluded.user.agents.list)",
          "propertyOrder" : 5960,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "httpOnly" : {
          "title" : "Http Only",
          "description" : "Flag saying whether HTTP only cookies are enabled. (property:
com.sun.identity.cookie.httponly)",
          "propertyOrder" : 5910,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "cdssoDomainList" : {
          "title" : "CDSSO Domain List",
          "description" : "Domains for which cookies have to be set in a CDSSO scenario. (property
name: org.forgerock.agents.jwt.cookie.domain.list)  <br> Example: <br> .sun.com",
          "propertyOrder" : 5800,
          "required" : false,
          "items" : {
            "type" : "string"
          },
```

```
          "type" : "array",
          "exampleValue" : ""
        },
        "authExchangeUri" : {
          "title" : "Authentication Exchange URI",
          "description" : "This property allows the administrator to enable an endpoint that will
facilitate the exchange of SSO tokens for OIDC JWTs. The value is empty by default and thus the
endpoint is not accessible. (property: org.forgerock.agents.authn.exchange.uri) (Agent 5.7+ only)",
          "propertyOrder" : 5901,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "setCookieAttributeMap" : {
          "title" : "Set-Cookie Attribute Map",
          "description" : "Text from this map will be added directly into the Set-Cookie header
by the AttributeTaskHandler and its decendents when it creates cookies out of Profile Attributes,
Session Info Attributes and/or Response Attributes. The key is the cookie name, the value is any
arbitrary text suitable for the Set-Cookie header. Users should remember semicolons if they wish
to add multiple values.  Values inappropriate for the header will likely cause the Agent to fail to
create the relevant cookie. (property: org.forgerock.agents.set.cookie.attribute.map)",
          "propertyOrder" : 5950,
          "required" : false,
          "patternProperties" : {
            ".*" : {
              "type" : "string"
            }
          },
          "type" : "object",
          "exampleValue" : ""
        },
        "acceptIPDPCookie" : {
          "title" : "Convert SSO Tokens into OpenID Connect JWTs",
          "description" : "When this property is set to true, for each incoming request, when the
user does not present a JWT in the designated cookie, the Agent will look for an SSO token in the
iPlanetDirectoryPro cookie (configurable in AM). If this is found, the Agent invokes AM to exchange
it for a JWT which is then used in further requests. The result is cached, so interaction with AM
will not be needed, if the same SSO token is presented in the future (and the existing cache entry is
still valid) (property: org.forgerock.agents.accept.ipdp.cookie.enabled)",
          "propertyOrder" : 5900,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "encodeCookies" : {
          "title" : "Encode Cookies",
          "description" : "Cookies are encoded, if set. (property: com.iplanet.am.cookie.encode)",
          "propertyOrder" : 5920,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "cookieResetDomains" : {
          "title" : "Cookies Reset Domain Map",
          "description" : "Maps cookie names specified in Cookie Reset Name List to value
being the domain of this cookie to be used when a reset event occurs. (property name:
org.forgerock.agents.cookie.reset.domain.map) ",
          "propertyOrder" : 4800,
          "required" : false,
```

```
          "patternProperties" : {
            ".*" : {
              "type" : "string"
            }
          },
          "type" : "object",
          "exampleValue" : ""
        },
        "cdssoSecureCookies" : {
          "title" : "CDSSO Secure Enable",
          "description" : "The SSO Token cookie set by the agent in the different domains in CDSSO
mode will be marked secure. Only transmitted if the communications channel with host is a secure one.
(property name: org.forgerock.agents.secure.cookies.enabled) ",
          "propertyOrder" : 5700,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "cdssoRedirectUri" : {
          "title" : "CDSSO Redirect URI",
          "description" : "An intermediate URI that is used by the Agent for processing CDSSO
requests. (property name: org.forgerock.agents.authn.redirect.uri) ",
          "propertyOrder" : 5100,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "cookieResetEnabled" : {
          "title" : "Cookie Reset",
          "description" : "Agent resets cookies in the response before redirecting to authentication.
(property name: org.forgerock.agents.cookie.reset.enabled) ",
          "propertyOrder" : 4600,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "cookieResetPaths" : {
          "title" : "Cookies Reset Path Map",
          "description" : "Maps cookie names specified in Cookie Reset Name List to value
being the path of this cookie to be used when a reset event occurs. (property name:
org.forgerock.agents.cookie.reset.path.map) ",
          "propertyOrder" : 4900,
          "required" : false,
          "patternProperties" : {
            ".*" : {
              "type" : "string"
            }
          },
          "type" : "object",
          "exampleValue" : ""
        },
        "authExchangeCookieName" : {
          "title" : "Authentication Exchange Cookie Name",
          "description" : "This property allows the administrator to define a cooke name that will be
used by the authn exchange endpoint. The value is empty by default and the endpoint will thus not be
capable of examining cookie values (property: org.forgerock.agents.authn.exchange.cookie.name) (Agent
5.7+ only)",
          "propertyOrder" : 5902,
          "required" : false,
```

```
          "type" : "string",
          "exampleValue" : ""
        },
        "cookieResetNames" : {
          "title" : "Cookies Reset Name List",
          "description" : "Cookie names that will be reset by the Agent if Cookie Reset is enabled.
(property name: org.forgerock.agents.cookie.reset.name.list) ",
          "propertyOrder" : 4700,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "secureCookies" : {
          "title" : "Secure Cookies",
          "description" : "On setting this property to true, all cookies created by the
Agent will be secure. The value is set to false for backwards compatibility. (property:
org.forgerock.agents.jwt.cookie.secure.enabled)",
          "propertyOrder" : 5930,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        }
      }
    },
    "advancedJ2EEAgentConfig" : {
      "type" : "object",
      "title" : "Advanced",
      "propertyOrder" : 5,
      "properties" : {
        "monitoringToCSV" : {
          "title" : "Export Monitoring Metrics to CSV",
          "description" : "When set to true, the Agent will write monitoring information to CSV files.
(property: org.forgerock.agents.monitoring.to.csv.enabled)",
          "propertyOrder" : 13085,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "customProperties" : {
          "title" : "Custom Properties",
          "description" : "Additional properties that allow users to augment the set of
properties supported by agent. (property name: com.sun.identity.agents.config.freeformproperties)
 <br> Examples: <br> customproperty=custom-value1 <br> customlist[0]=customlist-value-0
<br> customlist[1]=customlist-value-1 <br> custommap[key1]=custommap-value-1 <br>
custommap[key2]=custommap-value-2",
          "propertyOrder" : 20000,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "fragmentRelayUri" : {
          "title" : "Fragment Relay URI",
```

```
          "description" : "To enable unauthenticated fragment retention within incoming requests, set
 this property to a valid dummy URI within the Agent application.<br>Example: /agentapp/pre-authn-
fragment-capture <br>(property: org.forgerock.agents.authn.fragment.relay.uri) (Agent 5.7+ only)",
          "propertyOrder" : 13090,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "ssoExchangeCacheTTL" : {
          "title" : "Exchanged SSO Token Cache Time to Live",
          "description" : "This sets the time in minutes after which entries in the SSO token
 exchange cache will timeout and be purged.  Since exchanging SSO tokens for JWTs is an expensive
 process, previously exchanged SSO tokens are cached so that the roundtrip to AM can be avoided
 in the case where an entity is unable to permanently store its JWT in a cookie. (property:
 org.forgerock.agents.sso.exchange.cache.ttl.minutes) <br>Required Agent Restart",
          "propertyOrder" : 13900,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "clientIpHeader" : {
          "title" : "Client IP Address Header",
          "description" : "HTTP header name that holds the IP address of the client. (property name:
 org.forgerock.agents.http.header.containing.ip.address) ",
          "propertyOrder" : 1000,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "missingPostDataPreservationEntryUri" : {
          "title" : "Missing PDP entry URI",
          "description" : "An application-specific URI Map that is used in case the referenced
 PDP entry cannot be found in the local cache (due to ttl). In such cases it will redirect
 to the specified URI, otherwise it will show a HTTP 403 Forbidden error. (property name:
 org.forgerock.agents.pdp.noentry.url.map)<br>Examples: <br>To set a redirect target for application
 BankApp: enter Bankapp in Map Key field and enter a redirect URI in corresponding Map Value field.",
          "propertyOrder" : 13200,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "ssoExchangeCacheSize" : {
          "title" : "Exchanged SSO Token Cache Size",
          "description" : "The number of entries in the SSO Exchange cache. (property:
 org.forgerock.agents.sso.exchange.cache.size) <br>Required Agent Restart",
          "propertyOrder" : 13910,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "alternativeAgentHostname" : {
          "title" : "Alternative Agent Host Name",
          "description" : "Host name identifying the Agent protected server to the client browsers if
 different from the actual host name. (property name: org.forgerock.agents.agent.hostname) ",
          "propertyOrder" : 4100,
          "required" : false,
```

```
          "type" : "string",
          "exampleValue" : ""
        },
        "postDataCacheTtlMin" : {
          "title" : "PDP Cache TTL in Minutes",
          "description" : "This sets the time in minutes after which entries in the Post Data
Preservation cache will timeout and be purged. (property: org.forgerock.agents.pdp.cache.ttl.minutes)
<br>Required Agent Restart",
          "propertyOrder" : 13300,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "idleTimeRefreshWindow" : {
          "title" : "Idle Time Refresh Window",
          "description" : "Once every this number of minutes, the Agent will nudge AM so
it knows a particular session is still in use, thereby resetting its idle time. (property:
org.forgerock.agents.idle.time.window.minutes)",
          "propertyOrder" : 14200,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "postDataStickySessionMode" : {
          "title" : "PDP Stickysession mode",
          "description" : "If the PDP mechanism needs sticky loadbalancing, the URL mode
will append a querystring, while the Cookie mode will create a cookie. (property name:
org.forgerock.agents.pdp.sticky.session.mode)",
          "propertyOrder" : 13400,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "possibleXssCodeElements" : {
          "title" : "Possible XSS code elements",
          "description" : "If one of these strings occurs in the request, the client is redirected to
an error page. (property name: org.forgerock.agents.xss.code.element.list) ",
          "propertyOrder" : 12800,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "xssDetectionRedirectUri" : {
          "title" : "XSS detection redirect URI",
          "description" : "An application-specific Map that identifies a URI of the customized page if
XSS code has been deteced. (property name: org.forgerock.agents.xss.redirect.uri.map)  <br>Examples:
<br>To set a redirect target for application BankApp: enter BankApp in Map Key field, and enter a
redirect URI in Corresponding Map Value field.",
          "propertyOrder" : 12900,
          "required" : false,
          "patternProperties" : {
            ".*" : {
              "type" : "string"
            }
          },
          "type" : "object",
```

```
          "exampleValue" : ""
        },
        "postDataPreserveCacheEntryMaxTotalSizeMb" : {
          "title" : "PDP Maximum Cache Size",
          "description" : "Maximum size of the PDP cache, in megabytes (Property name:
org.forgerock.agents.pdp.cache.total.size.mb).",
          "propertyOrder" : 13600,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "policyClientPollingInterval" : {
          "title" : "Policy Cache TTL",
          "description" : "This sets the time in minutes after which entries in the policy cache will
timeout and be purged. (property name: org.forgerock.agents.policy.cache.ttl.minutes) <br>Required
Agent Restart",
          "propertyOrder" : 13950,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "clientHostnameHeader" : {
          "title" : "Client Hostname Header",
          "description" : "HTTP header name that holds the Hostname of the client. (property name:
org.forgerock.agents.http.header.containing.remote.hostname) ",
          "propertyOrder" : 1100,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "postDataPreserveCacheEntryMaxEntries" : {
          "title" : "PDP Maximum Number of Cache Entries",
          "description" : "Maximum number of entries to hold in the PDP cache (Property name:
org.forgerock.agents.pdp.cache.size).",
          "propertyOrder" : 13550,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "jwtCacheSize" : {
          "title" : "JWT Cache Size",
          "description" : "The maximum number of entries in the JWT cache. (property:
org.forgerock.agents.jwt.cache.size) <br>Required Agent Restart",
          "propertyOrder" : 13810,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "policyCacheSize" : {
          "title" : "Policy Cache Size",
          "description" : "The maximum number of sessions, i.e. distinct users, stored in the
policy evaluation cache at any one time. (property: org.forgerock.agents.policy.cache.session.size)
<br>Required Agent Restart",
          "propertyOrder" : 14000,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "postDataPreservation" : {
```

```
          "title" : "Post Data Preservation enabled",
          "description" : "Post Data Preservation functionality basically stores any POST
data before redirecting the user to the login screen and after successful login the agent
will generate a page that autosubmits the same POST to the original URL. (property name:
org.forgerock.agents.post.data.preservation.enabled)",
          "propertyOrder" : 13100,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "policyCachePerUser" : {
          "title" : "Policy Cache Per User",
          "description" : "This is the number of distinct policy evaluation entries that each session
(stored in the policy evaluation cache) can have.  Thus the total number of policy evaluation
results that can be stored is the \"Policy Cache Size\" multiplied by the \"Policy Cache Per User\".
(property: org.forgerock.agents.policy.cache.per.session.size) <br>Required Agent Restart",
          "propertyOrder" : 14100,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "alternativeAgentPort" : {
          "title" : "Alternative Agent Port Number",
          "description" : "Port number identifying the Agent protected server listening
port to the client browsers if different from the actual listening port. (property name:
org.forgerock.agents.agent.port) ",
          "propertyOrder" : 4200,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "postDataStickySessionKeyValue" : {
          "title" : "PDP Stickysession key-value",
          "description" : "The provided key-value pair will be used for adding to the URL or creating
the cookie. <br>Example: <br>Set 'lb=server1' to append to the querystring or to have 'lb' cookie
with 'server1' value. (property name: org.forgerock.agents.pdp.sticky.session.value)",
          "propertyOrder" : 13500,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "alternativeAgentProtocol" : {
          "title" : "Alternative Agent Protocol",
          "description" : "Protocol being used (http/https) by the client browsers to communicate with
the Agent protected server if different from the actual protocol used by the server. (property name:
org.forgerock.agents.agent.protocol) ",
          "propertyOrder" : 4300,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sessionCacheTTL" : {
          "title" : "Session Cache TTL",
          "description" : "This sets the time in minutes after which entries in the session cache
will timeout and be purged.  If an entry is not cached, the Agent will need to retrieve session
information from AM, hence by default the timeout is much longer than for the policy cache.
(property: org.forgerock.agents.session.cache.ttl.minutes) <br>Required Agent Restart",
          "propertyOrder" : 13700,
          "required" : false,
```

```
          "type" : "integer",
          "exampleValue" : ""
        },
        "jwtCacheTTL" : {
          "title" : "JWT Cache TTL",
          "description" : "This sets the time in minutes after which entries in the JWT cache will
 timeout and be purged.  Since all JWTs in the cache have been parsed, and parsing is a CPU intensive
 process, having a large timeout on this cache is advantageous and will save CPU cycles reparsing
 already seen JWTs (property: org.forgerock.agents.jwt.cache.ttl.minutes) <br>Required Agent Restart",
          "propertyOrder" : 13800,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "postDataCacheTtl" : {
          "title" : "PDP Cache TTL in Milliseconds",
          "description" : "This value tells how long a given POST entry should be stored in the
 local cache (in milliseconds), default value is 300000. DEPRECATED: use \"PDP Cache TTL in Minutes
\" instead (property name: com.sun.identity.agents.config.postdata.preserve.cache.entry.ttl)
 <br>Required Agent Restart",
          "propertyOrder" : 13310,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        }
      }
    }
  }
}
```


J2eeAgents

Realm Operations

Agents handler that is responsible for managing agents

Resource path: `/realm-config/agents/J2EEAgent`

Resource version: `1.0`

create

Usage:

```
am> create J2eeAgents --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "ssoJ2EEAgentConfig" : {
      "type" : "object",
      "title" : "SSO",
      "propertyOrder" : 2,
      "properties" : {
        "cookieResetPaths" : {
          "title" : "Cookies Reset Path Map",
          "description" : "Maps cookie names specified in Cookie Reset Name List to value
being the path of this cookie to be used when a reset event occurs. (property name:
org.forgerock.agents.cookie.reset.path.map) ",
          "propertyOrder" : 4900,
          "patternProperties" : {
            ".*" : {
              "type" : "string"
            }
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "object",
              "required" : false
            }
          }
        },
        "setCookieAttributeMap" : {
          "title" : "Set-Cookie Attribute Map",
          "description" : "Text from this map will be added directly into the Set-Cookie header
by the AttributeTaskHandler and its decendents when it creates cookies out of Profile Attributes,
Session Info Attributes and/or Response Attributes. The key is the cookie name, the value is any
arbitrary text suitable for the Set-Cookie header. Users should remember semicolons if they wish
to add multiple values.  Values inappropriate for the header will likely cause the Agent to fail to
create the relevant cookie. (property: org.forgerock.agents.set.cookie.attribute.map)",
          "propertyOrder" : 5950,
          "patternProperties" : {
            ".*" : {
              "type" : "string"
            }
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "object",
```

```
              "required" : false
            }
          }
        },
        "acceptIPDPCookie" : {
          "title" : "Convert SSO Tokens into OpenID Connect JWTs",
          "description" : "When this property is set to true, for each incoming request, when the
user does not present a JWT in the designated cookie, the Agent will look for an SSO token in the
iPlanetDirectoryPro cookie (configurable in AM). If this is found, the Agent invokes AM to exchange
it for a JWT which is then used in further requests. The result is cached, so interaction with AM
will not be needed, if the same SSO token is presented in the future (and the existing cache entry is
still valid) (property: org.forgerock.agents.accept.ipdp.cookie.enabled)",
          "propertyOrder" : 5900,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : false
            }
          }
        },
        "httpOnly" : {
          "title" : "Http Only",
          "description" : "Flag saying whether HTTP only cookies are enabled. (property:
com.sun.identity.cookie.httponly)",
          "propertyOrder" : 5910,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : false
            }
          }
        },
        "authExchangeCookieName" : {
          "title" : "Authentication Exchange Cookie Name",
          "description" : "This property allows the administrator to define a cooke name that will be
used by the authn exchange endpoint. The value is empty by default and the endpoint will thus not be
capable of examining cookie values (property: org.forgerock.agents.authn.exchange.cookie.name) (Agent
5.7+ only)",
          "propertyOrder" : 5902,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
```

```
              "type" : "string",
              "required" : false
            }
          }
        },
        "cdssoRedirectUri" : {
          "title" : "CDSSO Redirect URI",
          "description" : "An intermediate URI that is used by the Agent for processing CDSSO
requests. (property name: org.forgerock.agents.authn.redirect.uri) ",
          "propertyOrder" : 5100,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "cookieResetDomains" : {
          "title" : "Cookies Reset Domain Map",
          "description" : "Maps cookie names specified in Cookie Reset Name List to value
being the domain of this cookie to be used when a reset event occurs. (property name:
org.forgerock.agents.cookie.reset.domain.map) ",
          "propertyOrder" : 4800,
          "patternProperties" : {
            ".*" : {
              "type" : "string"
            }
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "object",
              "required" : false
            }
          }
        },
        "cdssoSecureCookies" : {
          "title" : "CDSSO Secure Enable",
          "description" : "The SSO Token cookie set by the agent in the different domains in CDSSO
mode will be marked secure. Only transmitted if the communications channel with host is a secure one.
(property name: org.forgerock.agents.secure.cookies.enabled) ",
          "propertyOrder" : 5700,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
```

```
            },
            "value" : {
              "type" : "boolean",
              "required" : false
            }
          }
        },
        "authExchangeUri" : {
          "title" : "Authentication Exchange URI",
          "description" : "This property allows the administrator to enable an endpoint that will
facilitate the exchange of SSO tokens for OIDC JWTs. The value is empty by default and thus the
endpoint is not accessible. (property: org.forgerock.agents.authn.exchange.uri) (Agent 5.7+ only)",
          "propertyOrder" : 5901,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "setCookieInternalMap" : {
          "title" : "Set-Cookie Internal Map",
          "description" : "Text from this map will be added directly into the Set-Cookie header
when creating \"internal\" cookies (e.g. the am-auth-jwt and pre-auth cookies). This allows, among
other things, the same-site value to be manipulated. The key is the cookie name, the value is any
arbitrary text suitable for the Set-Cookie header. Users should remember semicolons if they wish
to add multiple values.  Values inappropriate for the header will likely cause the Agent to fail to
create the relevant cookie. (property: org.forgerock.agents.set.cookie.internal.map)",
          "propertyOrder" : 5940,
          "patternProperties" : {
            ".*" : {
              "type" : "string"
            }
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "object",
              "required" : false
            }
          }
        },
        "secureCookies" : {
          "title" : "Secure Cookies",
          "description" : "On setting this property to true, all cookies created by the
Agent will be secure. The value is set to false for backwards compatibility. (property:
org.forgerock.agents.jwt.cookie.secure.enabled)",
          "propertyOrder" : 5930,
```

```
        "type" : "object",
        "exampleValue" : "",
        "properties" : {
          "inherited" : {
            "type" : "boolean",
            "required" : true
          },
          "value" : {
            "type" : "boolean",
            "required" : false
          }
        }
      },
      "cookieResetEnabled" : {
        "title" : "Cookie Reset",
        "description" : "Agent resets cookies in the response before redirecting to authentication.
(property name: org.forgerock.agents.cookie.reset.enabled) ",
        "propertyOrder" : 4600,
        "type" : "object",
        "exampleValue" : "",
        "properties" : {
          "inherited" : {
            "type" : "boolean",
            "required" : true
          },
          "value" : {
            "type" : "boolean",
            "required" : false
          }
        }
      },
      "cdssoDomainList" : {
        "title" : "CDSSO Domain List",
        "description" : "Domains for which cookies have to be set in a CDSSO scenario. (property
name: org.forgerock.agents.jwt.cookie.domain.list)  <br> Example: <br> .sun.com",
        "propertyOrder" : 5800,
        "items" : {
          "type" : "string"
        },
        "type" : "object",
        "exampleValue" : "",
        "properties" : {
          "inherited" : {
            "type" : "boolean",
            "required" : true
          },
          "value" : {
            "type" : "array",
            "required" : false
          }
        }
      },
      "cookieResetNames" : {
        "title" : "Cookies Reset Name List",
        "description" : "Cookie names that will be reset by the Agent if Cookie Reset is enabled.
(property name: org.forgerock.agents.cookie.reset.name.list) ",
        "propertyOrder" : 4700,
        "items" : {
          "type" : "string"
```

```
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "array",
              "required" : false
            }
          }
        },
        "excludedUserAgentsList" : {
          "title" : "Samesite Cookie Attributes Excluded User Agents Pattern List",
          "description" : "Excluded User agents pattern list. List of incompatible
user agents that will be prevented from receiving SameSite cookie attributes. <br>
(Property:org.forgerock.agents.samesite.excluded.user.agents.list)",
          "propertyOrder" : 5960,
          "items" : {
            "type" : "string"
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "array",
              "required" : false
            }
          }
        },
        "encodeCookies" : {
          "title" : "Encode Cookies",
          "description" : "Cookies are encoded, if set. (property: com.iplanet.am.cookie.encode)",
          "propertyOrder" : 5920,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : false
            }
          }
        }
      }
    },
    "advancedJ2EEAgentConfig" : {
      "type" : "object",
      "title" : "Advanced",
      "propertyOrder" : 5,
```

```
     "properties" : {
       "postDataStickySessionMode" : {
         "title" : "PDP Stickysession mode",
         "description" : "If the PDP mechanism needs sticky loadbalancing, the URL mode
will append a querystring, while the Cookie mode will create a cookie. (property name:
org.forgerock.agents.pdp.sticky.session.mode)",
         "propertyOrder" : 13400,
         "type" : "object",
         "exampleValue" : "",
         "properties" : {
           "inherited" : {
             "type" : "boolean",
             "required" : true
           },
           "value" : {
             "type" : "string",
             "required" : false
           }
         }
       },
       "alternativeAgentHostname" : {
         "title" : "Alternative Agent Host Name",
         "description" : "Host name identifying the Agent protected server to the client browsers if
different from the actual host name. (property name: org.forgerock.agents.agent.hostname) ",
         "propertyOrder" : 4100,
         "type" : "object",
         "exampleValue" : "",
         "properties" : {
           "inherited" : {
             "type" : "boolean",
             "required" : true
           },
           "value" : {
             "type" : "string",
             "required" : false
           }
         }
       },
       "postDataCacheTtlMin" : {
         "title" : "PDP Cache TTL in Minutes",
         "description" : "This sets the time in minutes after which entries in the Post Data
Preservation cache will timeout and be purged. (property: org.forgerock.agents.pdp.cache.ttl.minutes)
<br>Required Agent Restart",
         "propertyOrder" : 13300,
         "type" : "object",
         "exampleValue" : "",
         "properties" : {
           "inherited" : {
             "type" : "boolean",
             "required" : true
           },
           "value" : {
             "type" : "integer",
             "required" : false
           }
         }
       },
       "ssoExchangeCacheTTL" : {
         "title" : "Exchanged SSO Token Cache Time to Live",
```

```
          "description" : "This sets the time in minutes after which entries in the SSO token
exchange cache will timeout and be purged.  Since exchanging SSO tokens for JWTs is an expensive
process, previously exchanged SSO tokens are cached so that the roundtrip to AM can be avoided
in the case where an entity is unable to permanently store its JWT in a cookie. (property:
org.forgerock.agents.sso.exchange.cache.ttl.minutes) <br>Required Agent Restart",
          "propertyOrder" : 13900,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "integer",
              "required" : false
            }
          }
        },
        "clientHostnameHeader" : {
          "title" : "Client Hostname Header",
          "description" : "HTTP header name that holds the Hostname of the client. (property name:
org.forgerock.agents.http.header.containing.remote.hostname) ",
          "propertyOrder" : 1100,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "xssDetectionRedirectUri" : {
          "title" : "XSS detection redirect URI",
          "description" : "An application-specific Map that identifies a URI of the customized page if
XSS code has been deteced. (property name: org.forgerock.agents.xss.redirect.uri.map)  <br>Examples:
<br>To set a redirect target for application BankApp: enter BankApp in Map Key field, and enter a
redirect URI in Corresponding Map Value field.",
          "propertyOrder" : 12900,
          "patternProperties" : {
            ".*" : {
              "type" : "string"
            }
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "object",
              "required" : false
```

```
            }
          }
        },
        "ssoExchangeCacheSize" : {
          "title" : "Exchanged SSO Token Cache Size",
          "description" : "The number of entries in the SSO Exchange cache. (property:
org.forgerock.agents.sso.exchange.cache.size) <br>Required Agent Restart",
          "propertyOrder" : 13910,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "integer",
              "required" : false
            }
          }
        },
        "customProperties" : {
          "title" : "Custom Properties",
          "description" : "Additional properties that allow users to augment the set of
properties supported by agent. (property name: com.sun.identity.agents.config.freeformproperties)
 <br> Examples: <br> customproperty=custom-value1 <br> customlist[0]=customlist-value-0
<br> customlist[1]=customlist-value-1 <br> custommap[key1]=custommap-value-1 <br>
custommap[key2]=custommap-value-2",
          "propertyOrder" : 20000,
          "items" : {
            "type" : "string"
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "array",
              "required" : false
            }
          }
        },
        "postDataPreserveCacheEntryMaxEntries" : {
          "title" : "PDP Maximum Number of Cache Entries",
          "description" : "Maximum number of entries to hold in the PDP cache (Property name:
org.forgerock.agents.pdp.cache.size).",
          "propertyOrder" : 13550,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "integer",
```

```
              "required" : false
            }
          }
        },
        "postDataPreservation" : {
          "title" : "Post Data Preservation enabled",
          "description" : "Post Data Preservation functionality basically stores any POST
data before redirecting the user to the login screen and after successful login the agent
will generate a page that autosubmits the same POST to the original URL. (property name:
org.forgerock.agents.post.data.preservation.enabled)",
          "propertyOrder" : 13100,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : false
            }
          }
        },
        "monitoringToCSV" : {
          "title" : "Export Monitoring Metrics to CSV",
          "description" : "When set to true, the Agent will write monitoring information to CSV files.
(property: org.forgerock.agents.monitoring.to.csv.enabled)",
          "propertyOrder" : 13085,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : false
            }
          }
        },
        "idleTimeRefreshWindow" : {
          "title" : "Idle Time Refresh Window",
          "description" : "Once every this number of minutes, the Agent will nudge AM so
it knows a particular session is still in use, thereby resetting its idle time. (property:
org.forgerock.agents.idle.time.window.minutes)",
          "propertyOrder" : 14200,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "integer",
              "required" : false
            }
```

```
        }
      },
      "clientIpHeader" : {
        "title" : "Client IP Address Header",
        "description" : "HTTP header name that holds the IP address of the client. (property name:
org.forgerock.agents.http.header.containing.ip.address) ",
        "propertyOrder" : 1000,
        "type" : "object",
        "exampleValue" : "",
        "properties" : {
          "inherited" : {
            "type" : "boolean",
            "required" : true
          },
          "value" : {
            "type" : "string",
            "required" : false
          }
        }
      },
      "policyCachePerUser" : {
        "title" : "Policy Cache Per User",
        "description" : "This is the number of distinct policy evaluation entries that each session
(stored in the policy evaluation cache) can have.  Thus the total number of policy evaluation
results that can be stored is the \"Policy Cache Size\" multiplied by the \"Policy Cache Per User\".
(property: org.forgerock.agents.policy.cache.per.session.size) <br>Required Agent Restart",
        "propertyOrder" : 14100,
        "type" : "object",
        "exampleValue" : "",
        "properties" : {
          "inherited" : {
            "type" : "boolean",
            "required" : true
          },
          "value" : {
            "type" : "integer",
            "required" : false
          }
        }
      },
      "alternativeAgentPort" : {
        "title" : "Alternative Agent Port Number",
        "description" : "Port number identifying the Agent protected server listening
port to the client browsers if different from the actual listening port. (property name:
org.forgerock.agents.agent.port) ",
        "propertyOrder" : 4200,
        "type" : "object",
        "exampleValue" : "",
        "properties" : {
          "inherited" : {
            "type" : "boolean",
            "required" : true
          },
          "value" : {
            "type" : "string",
            "required" : false
          }
        }
      },
```

```
        "postDataPreserveCacheEntryMaxTotalSizeMb" : {
          "title" : "PDP Maximum Cache Size",
          "description" : "Maximum size of the PDP cache, in megabytes (Property name:
 org.forgerock.agents.pdp.cache.total.size.mb).",
          "propertyOrder" : 13600,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "integer",
              "required" : false
            }
          }
        },
        "policyCacheSize" : {
          "title" : "Policy Cache Size",
          "description" : "The maximum number of sessions, i.e. distinct users, stored in the
 policy evaluation cache at any one time. (property: org.forgerock.agents.policy.cache.session.size)
 <br>Required Agent Restart",
          "propertyOrder" : 14000,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "integer",
              "required" : false
            }
          }
        },
        "fragmentRelayUri" : {
          "title" : "Fragment Relay URI",
          "description" : "To enable unauthenticated fragment retention within incoming requests, set
 this property to a valid dummy URI within the Agent application.<br>Example: /agentapp/pre-authn-
fragment-capture <br>(property: org.forgerock.agents.authn.fragment.relay.uri) (Agent 5.7+ only)",
          "propertyOrder" : 13090,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "alternativeAgentProtocol" : {
          "title" : "Alternative Agent Protocol",
```

```
          "description" : "Protocol being used (http/https) by the client browsers to communicate with
the Agent protected server if different from the actual protocol used by the server. (property name:
org.forgerock.agents.agent.protocol) ",
          "propertyOrder" : 4300,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "postDataStickySessionKeyValue" : {
          "title" : "PDP Stickysession key-value",
          "description" : "The provided key-value pair will be used for adding to the URL or creating
the cookie. <br>Example: <br>Set 'lb=server1' to append to the querystring or to have 'lb' cookie
with 'server1' value. (property name: org.forgerock.agents.pdp.sticky.session.value)",
          "propertyOrder" : 13500,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "missingPostDataPreservationEntryUri" : {
          "title" : "Missing PDP entry URI",
          "description" : "An application-specific URI Map that is used in case the referenced
PDP entry cannot be found in the local cache (due to ttl). In such cases it will redirect
to the specified URI, otherwise it will show a HTTP 403 Forbidden error. (property name:
org.forgerock.agents.pdp.noentry.url.map)<br>Examples: <br>To set a redirect target for application
BankApp: enter Bankapp in Map Key field and enter a redirect URI in corresponding Map Value field.",
          "propertyOrder" : 13200,
          "items" : {
            "type" : "string"
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "array",
              "required" : false
            }
          }
```

```
        },
        "sessionCacheTTL" : {
          "title" : "Session Cache TTL",
          "description" : "This sets the time in minutes after which entries in the session cache
 will timeout and be purged.  If an entry is not cached, the Agent will need to retrieve session
 information from AM, hence by default the timeout is much longer than for the policy cache.
 (property: org.forgerock.agents.session.cache.ttl.minutes) <br>Required Agent Restart",
          "propertyOrder" : 13700,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "integer",
              "required" : false
            }
          }
        },
        "postDataCacheTtl" : {
          "title" : "PDP Cache TTL in Milliseconds",
          "description" : "This value tells how long a given POST entry should be stored in the
 local cache (in milliseconds), default value is 300000. DEPRECATED: use \"PDP Cache TTL in Minutes
\" instead (property name: com.sun.identity.agents.config.postdata.preserve.cache.entry.ttl)
 <br>Required Agent Restart",
          "propertyOrder" : 13310,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "integer",
              "required" : false
            }
          }
        },
        "policyClientPollingInterval" : {
          "title" : "Policy Cache TTL",
          "description" : "This sets the time in minutes after which entries in the policy cache will
 timeout and be purged. (property name: org.forgerock.agents.policy.cache.ttl.minutes) <br>Required
 Agent Restart",
          "propertyOrder" : 13950,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "integer",
              "required" : false
            }
          }
```

```
      },
      "jwtCacheTTL" : {
        "title" : "JWT Cache TTL",
        "description" : "This sets the time in minutes after which entries in the JWT cache will
timeout and be purged.  Since all JWTs in the cache have been parsed, and parsing is a CPU intensive
process, having a large timeout on this cache is advantageous and will save CPU cycles reparsing
already seen JWTs (property: org.forgerock.agents.jwt.cache.ttl.minutes) <br>Required Agent Restart",
        "propertyOrder" : 13800,
        "type" : "object",
        "exampleValue" : "",
        "properties" : {
          "inherited" : {
            "type" : "boolean",
            "required" : true
          },
          "value" : {
            "type" : "integer",
            "required" : false
          }
        }
      },
      "possibleXssCodeElements" : {
        "title" : "Possible XSS code elements",
        "description" : "If one of these strings occurs in the request, the client is redirected to
an error page. (property name: org.forgerock.agents.xss.code.element.list) ",
        "propertyOrder" : 12800,
        "items" : {
          "type" : "string"
        },
        "type" : "object",
        "exampleValue" : "",
        "properties" : {
          "inherited" : {
            "type" : "boolean",
            "required" : true
          },
          "value" : {
            "type" : "array",
            "required" : false
          }
        }
      },
      "jwtCacheSize" : {
        "title" : "JWT Cache Size",
        "description" : "The maximum number of entries in the JWT cache. (property:
org.forgerock.agents.jwt.cache.size) <br>Required Agent Restart",
        "propertyOrder" : 13810,
        "type" : "object",
        "exampleValue" : "",
        "properties" : {
          "inherited" : {
            "type" : "boolean",
            "required" : true
          },
          "value" : {
            "type" : "integer",
            "required" : false
          }
        }
```

```
        }
      }
    },
    "miscJ2EEAgentConfig" : {
      "type" : "object",
      "title" : "Miscellaneous",
      "propertyOrder" : 4,
      "properties" : {
        "gotoUrl" : {
          "title" : "Goto Url",
          "description" : "This is a URL used in rare circumstances where the Agent has nowhere
else to go.  For instance if the user requests a resource, authenticates for the first time,
then presses the back button and the administrator hasn't set up the authn fail URL. (property:
org.forgerock.agents.default.goto.url)",
          "propertyOrder" : 19200,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "unwantedHttpUrlParams" : {
          "title" : "Remove Query Parameters",
          "description" : "Specifies a list of query parameters to be removed from a URL for policy
decision and caching purposes. The property has the format [Domain/path] | parameter[,parameter...]
with no spaces between values (property: org.forgerock.agents.unwanted.http.url.param.list)
<br>Example: myapp.example.com/customers|location,lang",
          "propertyOrder" : 19500,
          "items" : {
            "type" : "string"
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "array",
              "required" : false
            }
          }
        },
        "loginReasonParameterName" : {
          "title" : "Login Reason Parameter Name",
          "description" : "Property to say why the user is being asked to login, the agent will (in
custom login mode ONLY) pass the named parameter to the custom login endpoint, with an appropriate
value.  Note that this property is not enabled by default as this additional information represents
an information leak. Default reasons: NO_TOKEN, JWT_INVALID, TOKEN_EXPIRED, EXCEPTION. (property:
org.forgerock.agents.login.reason.parameter.name)",
          "propertyOrder" : 18700,
```

```
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "authFailReasonParameterRemapper" : {
          "title" : "Authentication Fail Reason Parameter Value Map",
          "description" : "This map allows some of the possible reasons to be
mapped to arbitrary values. When empty, will use default values. (property:
org.forgerock.agents.authn.fail.reason.remapper)",
          "propertyOrder" : 19100,
          "patternProperties" : {
            ".*" : {
              "type" : "string"
            }
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "object",
              "required" : false
            }
          }
        },
        "gotoParameterName" : {
          "title" : "Goto Parameter Name",
          "description" : "This is the name of the HTTP query \"goto\" parameter. It is not
recommended to change it. (property name: com.sun.identity.agents.config.redirect.param) ",
          "propertyOrder" : 3600,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "localeCountry" : {
          "title" : "Locale Country",
          "description" : "(property name: org.forgerock.agents.locale.country) <br>Required Agent
Restart",
```

```
          "propertyOrder" : 1400,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "authFailReasonParameterName" : {
          "title" : "Authentication Fail Reason Parameter Name",
          "description" : "If this property is defined, the agent will pass the named parameter
 to a custom page (defined by \"Authentication Fail Reason Url\") saying why authentication
 failed.  The reason can be very detailed and users may want to use the \"Authentication
 Fail Reason Parameter Value Map\" to give custom detail, otherwise these default values
 will be used: AUTHN_BOOKKEEPING_COOKIE_MISSING, NONCE_MISSING, EXCEPTION (property:
 org.forgerock.agents.authn.fail.reason.parameter.name)",
          "propertyOrder" : 19000,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "wantedHttpUrlParams" : {
          "title" : "Retain Query Parameters",
          "description" : "Specifies a list of query parameters to be retained (other parameters
 will be removed) from a URL for policy decision and caching purposes. The property has the
 format [Domain/path] | parameter[,parameter...] with no spaces between values. (property:
 org.forgerock.agents.wanted.http.url.param.list) <br>Example: myapp.example.com/customers|
location,lang",
          "propertyOrder" : 19300,
          "items" : {
            "type" : "string"
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "array",
              "required" : false
            }
          }
```

```
        },
        "loginReasonMap" : {
          "title" : "Login Reason Value Map",
          "description" : "This map allows some of the possible reasons to be mapped to
 arbitrary values, when empty will be used default values(see: \"Login Reason Parameter Name
\" description). LOGIN REASON=CUSTOM VALUE e.g. [JWT_INVALID]=corrupted_token. (property:
 org.forgerock.agents.login.reason.remapper)",
          "propertyOrder" : 18800,
          "patternProperties" : {
            ".*" : {
              "type" : "string"
            }
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "object",
              "required" : false
            }
          }
        },
        "legacyUserAgentSupport" : {
          "title" : "Legacy User Agent Support Enable",
          "description" : "Enables support for legacy user agents (browser). (property name:
 org.forgerock.agents.legacy.support.enabled) ",
          "propertyOrder" : 6700,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : false
            }
          }
        },
        "serviceResolverClass" : {
          "title" : "Service Resolver Class Name",
          "description" : "Name of the service resolver class to change in order
 to instantiate own service resolver and overriding default ones <br>(property:
 org.forgerock.agents.service.resolver.class.name) (Agent 5.6.2+ only) <br> Agent restart is
 required",
          "propertyOrder" : 19700,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
```

```
              "type" : "string",
              "required" : false
            }
          }
        },
        "wantedHttpUrlRegexParams" : {
          "title" : "Regular Expression Retain Query Parameters",
          "description" : "Specifies a list of regular expressions the agent uses to match query
parameters to be retained for policy decision and caching purposes. The property has the format
[Domain/path] | regular_expression[,regular_expression...] with no spaces between values. (property:
org.forgerock.agents.wanted.http.url.params.regex.list)",
          "propertyOrder" : 19400,
          "items" : {
            "type" : "string"
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "array",
              "required" : false
            }
          }
        },
        "authFailReasonUrl" : {
          "title" : "Authentication Fail Reason Url",
          "description" : "This property allows administrators to set the URL/URI of a web page that
says that authentication failed and which may, using the login fail reason parameter, explain why.
(property: org.forgerock.agents.authn.fail.url)",
          "propertyOrder" : 18900,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "portCheckEnabled" : {
          "title" : "Port Check Enable",
          "description" : "Indicates if port check functionality is enabled or disabled. (property
name: org.forgerock.agents.port.check.enabled) ",
          "propertyOrder" : 7200,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
```

```
            "value" : {
              "type" : "boolean",
              "required" : false
            }
          }
        },
        "legacyRedirectUri" : {
          "title" : "Legacy User Agent Redirect URI",
          "description" : "An intermediate URI used by the Agent to redirect legacy user agent
requests. (property name: org.forgerock.agents.legacy.redirect.uri) ",
          "propertyOrder" : 6900,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "portCheckSetting" : {
          "title" : "Port Check Setting",
          "description" : "Map of port versus protocol entries with the key being the listening port
number and value being the listening protocol to be used by the Agent to identify requests with
invalid port numbers. (property name: org.forgerock.agents.port.check.map)  <br> Example: <br> To
map port 80 to protocol http: enter 80 in Map Key field, and enter http in Corresponding Map Value
field.",
          "propertyOrder" : 7400,
          "patternProperties" : {
            ".*" : {
              "type" : "string"
            }
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "object",
              "required" : false
            }
          }
        },
        "unwantedHttpUrlRegexParams" : {
          "title" : "Regular Expression Remove Query Parameters",
          "description" : "Specifies a list of regular expressions the agent uses to match query
parameters to be removed from a URL for policy decision and caching purposes. The property has the
format [Domain/path] | regular_expression[,regular_expression...] with no spaces between values.
(property: org.forgerock.agents.unwanted.http.url.params.regex.list)",
          "propertyOrder" : 19600,
          "items" : {
            "type" : "string"
```

```
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "array",
              "required" : false
            }
          }
        },
        "legacyUserAgentList" : {
          "title" : "Legacy User Agent List",
          "description" : "List of user agent header values that identify legacy
browsers. Entries in this list can have wild card character '*'. (property name:
org.forgerock.agents.legacy.user.agent.list) ",
          "propertyOrder" : 6800,
          "items" : {
            "type" : "string"
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "array",
              "required" : false
            }
          }
        },
        "portCheckFile" : {
          "title" : "Port Check File",
          "description" : "Name or complete path of a file that has the necessary content needed to
handle requests that need port correction. (property name: org.forgerock.agents.port.check.file) ",
          "propertyOrder" : 7300,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "ignorePathInfo" : {
          "title" : "Ignore Path Info in Request URL",
          "description" : "The path info will be stripped from the request URL while doing Not
Enforced List check and url policy evaluation if the value is set to true. (property name:
com.sun.identity.agents.config.ignore.path.info)",
```

```
          "propertyOrder" : 18600,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : false
            }
          }
        },
        "localeLanguage" : {
          "title" : "Locale Language",
          "description" : "(property name: org.forgerock.agents.locale.language) <br>Required Agent
Restart",
          "propertyOrder" : 1300,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        }
      }
    },
    "applicationJ2EEAgentConfig" : {
      "type" : "object",
      "title" : "Application",
      "propertyOrder" : 1,
      "properties" : {
        "profileAttributeFetchMode" : {
          "title" : "Profile Attribute Fetch Mode",
          "description" : "The mode of fetching profile attributes. (property name:
com.sun.identity.agents.config.profile.attribute.fetch.mode) ",
          "propertyOrder" : 8700,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "logoutRequestParameters" : {
          "title" : "Logout Request Parameter",
```

```
          "description" : "An application-specific Map that identifies a parameter
which when present in the HTTP request indicates a logout event. (property name:
org.forgerock.agents.logout.request.param.map)  <br>Valid key: the web application name. <br>Valid
value: the logout request parameter. <br>For this property, a global value can be set to apply to
all the applications that don't have their own specific logout request parameter.   <br> Examples:
<br>To set a global application logout request parameter: leave Map Key field empty, and enter the
global application logout request parameter logoutparam in Corresponding Map Value field. <br> To set
the logout request parameter for application BankApp: enter BankApp in Map Key field, and enter the
logout request parameter logoutparam in Corresponding Map Value field.",
          "propertyOrder" : 6100,
          "patternProperties" : {
            ".*" : {
              "type" : "string"
            }
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "object",
              "required" : false
            }
          }
        },
        "invertNotEnforcedIps" : {
          "title" : "Invert Not Enforced IPs",
          "description" : "Client IP Addresses to invert protection of IP
addresses listed in the related Not Enforced Client IP List. (property name:
org.forgerock.agents.notenforced.ip.invert.enabled) ",
          "propertyOrder" : 8000,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : false
            }
          }
        },
        "notEnforcedIps" : {
          "title" : "Not Enforced Client IP List",
          "description" : "No authentication and authorization protection from agent
are required for the requests coming from these client IP addresses. (property name:
org.forgerock.agents.notenforced.ip.list)  <br> Examples: <br> 192.18.145.* <br> 192.18.146.123",
          "propertyOrder" : 7900,
          "items" : {
            "type" : "string"
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
```

```
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "array",
              "required" : false
            }
          }
        },
        "continuousSecurityCookies" : {
          "title" : "Continuous Security Cookies",
          "description" : "The name of the cookies to be sent as part of the payload during policy
 evaluation, which can be accessed via the 'environment' variable in a policy script. The 'key' is
 the name of the cookie to be sent, and the 'value' is the name which it will appear as in the policy
 evaluation script. It is possible to map multiple cookies to the same name (they will simply appear
 as an array in the evaluation script). If the cookie doesn't exist, then the empty string will be
 sent.",
          "propertyOrder" : 3210,
          "patternProperties" : {
            ".*" : {
              "type" : "string"
            }
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "object",
              "required" : false
            }
          }
        },
        "applicationLogoutUris" : {
          "title" : "Application Logout URI",
          "description" : "An application-specific Map that identifies a request URI which indicates
 a logout event. (property name: org.forgerock.agents.logout.endpoint.map) <br>Valid key: the web
 application name. <br>Valid value: the application logout URI. <br>For this property, a global value
 can be set to apply to all the applications that don't have their own specific logout URI.  <br>
 Examples: <br>To set a global application logout URI: leave Map Key field empty, and enter the global
 application logout URI /logout.jsp in Corresponding Map Value field. <br> To set the logout URI for
 application BankApp: enter BankApp in Map Key field, and enter the application logout URI /BankApp/
logout.jsp in Corresponding Map Value field.",
          "propertyOrder" : 6000,
          "patternProperties" : {
            ".*" : {
              "type" : "string"
            }
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
```

```
            },
            "value" : {
              "type" : "object",
              "required" : false
            }
          }
        },
        "sessionAttributeFetchMode" : {
          "title" : "Session Attribute Fetch Mode",
          "description" : "The mode of fetching session attributes. (property name:
com.sun.identity.agents.config.session.attribute.fetch.mode) ",
          "propertyOrder" : 8900,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "notEnforcedIpsCacheEnabled" : {
          "title" : "Not Enforced IP Cache Flag",
          "description" : "Enable caching of not-enforced IP list evaluation results. (property name:
org.forgerock.agents.notenforced.ip.cache.enabled) ",
          "propertyOrder" : 8100,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : false
            }
          }
        },
        "cookieAttributeUrlEncoded" : {
          "title" : "Attribute Cookie Encode",
          "description" : "Indicates if the value of the attribute should be URL encoded before being
set as a cookie. (property name: org.forgerock.agents.attribute.cookie.encode.enabled) ",
          "propertyOrder" : 8500,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : false
            }
```

```
          }
        },
        "logoutEntryUri" : {
          "title" : "Logout Entry URI",
          "description" : "An application-specific Map that identifies a URI to be used as an entry
 point after successful logout and subsequent successful authentication if applicable. (property name:
 org.forgerock.agents.logout.goto.map) <br>Valid key: the web application name. <br>Valid value: the
 logout entry URI. <br>For this property, a global value can be set to apply to all the applications
 that don't have their own specific logout entry URI.   <br> Examples: <br>To set a global application
 logout entry URI: leave Map Key field empty, and enter the global application logout entry URI /
welcome.html in Corresponding Map Value field. <br> To set the logout entry URI for application
 BankApp: enter BankApp in Map Key field, and enter the logout entry URI /BankApp/welcome.html in
 Corresponding Map Value field.",
          "propertyOrder" : 6300,
          "patternProperties" : {
            ".*" : {
              "type" : "string"
            }
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "object",
              "required" : false
            }
          }
        },
        "cookieAttributeMultiValueSeparator" : {
          "title" : "Cookie Separator Character",
          "description" : "Character that will be used to separate multiple
 values of the same attribute when it is being set as a cookie. (property name:
 org.forgerock.agents.attribute.cookie.separator) ",
          "propertyOrder" : 8300,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "responseAttributeFetchMode" : {
          "title" : "Response Attribute Fetch Mode",
          "description" : "The mode of fetching policy response attributes. (property name:
 com.sun.identity.agents.config.response.attribute.fetch.mode) ",
          "propertyOrder" : 9100,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
```

```
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "notEnforcedIpsCacheSize" : {
          "title" : "Not Enforced IP Cache Size",
          "description" : "Size of the cache to be used if Not Enforced IP Cache Flag is enabled.
(property name: org.forgerock.agents.notenforced.ip.cache.size) ",
          "propertyOrder" : 8200,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "integer",
              "required" : false
            }
          }
        },
        "notEnforcedFavicon" : {
          "title" : "Not Enforced Favicon",
          "description" : "This flag, if enabled, automatically adds \"*/favicon.ico\" to
the not enforced list.  This can help to avoid odd situations in which a user is required to
log in after logging out, just because favicon.ico has been requested by browser. (property:
org.forgerock.agents.auto.not.enforce.favicon.enabled) <br>Required Agent Restart",
          "propertyOrder" : 7650,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : false
            }
          }
        },
        "notEnforcedRuleCompoundSeparator" : {
          "title" : "Not Enforced Compound Rule Separator",
          "description" : "Specifies a separator for not enforced compound rules. The format for
compound rules requires a list of IP rules, a separator (by default the | character), and a list of
URI rules. <br>Example, GET 192.168.1.1-192.168.4.3 | /images/* <br>Configure a different separator
(for example, &&) when working with the REGEX keyword to avoid invalid regular expressions.",
          "propertyOrder" : 7450,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
```

```
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "resourceAccessDeniedUri" : {
          "title" : "Resource Access Denied URI",
          "description" : "An application-specific Map that identifies a URI of the customized access
denied page. (property name: org.forgerock.agents.access.denied.uri.map) <br>Valid key: the web
application name. <br>Valid value: the customized application access denied page URI. <br>For this
property, a global value can be set to apply to all the applications that don't have their own
specific access denied page.  <br> Examples: <br>To set a global access denied page: leave Map Key
field empty, and enter the global access denied page URI /sample/accessdenied.html in Corresponding
Map Value field. <br> To set the access denied page URI for application BankApp: enter BankApp
in Map Key field, and enter the application access denied page URI /BankApp/accessdenied.html in
Corresponding Map Value field.",
          "propertyOrder" : 2700,
          "patternProperties" : {
            ".*" : {
              "type" : "string"
            }
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "object",
              "required" : false
            }
          }
        },
        "profileAttributeMap" : {
          "title" : "Profile Attribute Mapping",
          "description" : "Maps the profile attributes to be populated under specific names for the
currently authenticated user. (property name: org.forgerock.agents.profile.attribute.map)  <br>
Example: <br> To populate the value of profile attribute cn under name CUSTOM-Common-Name: enter cn
in Map Key field, and enter CUSTOM-Common-Name in Corresponding Map Value field. <br> To populate
the value of profile attribute mail under name CUSTOM-Email: enter mail in Map Key field, and enter
CUSTOM-Email in Corresponding Map Value field.",
          "propertyOrder" : 8800,
          "patternProperties" : {
            ".*" : {
              "type" : "string"
            }
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
```

```
            },
            "value" : {
              "type" : "object",
              "required" : false
            }
          }
        },
        "headerAttributeDateFormat" : {
          "title" : "Fetch Attribute Date Format",
          "description" : "Format of date attribute values to be used when the attribute is
 being set as HTTP header. Format is based on java.text.SimpleDateFormat. (property name:
 org.forgerock.agents.attribute.date.format) ",
          "propertyOrder" : 8400,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "notEnforcedUris" : {
          "title" : "Not Enforced URIs",
          "description" : "List of URIs for which protection is not enforced by the Agent. (property
 name: org.forgerock.agents.notenforced.uri.list)  <br> Examples: <br> /BankApp/public/* <br> /
BankApp/images/*",
          "propertyOrder" : 7500,
          "items" : {
            "type" : "string"
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "array",
              "required" : false
            }
          }
        },
        "responseAttributeMap" : {
          "title" : "Response Attribute Mapping",
          "description" : "Maps the policy response attributes to be populated under specific names
 for the currently authenticated user. (property name: org.forgerock.agents.response.attribute.map)
 <br> Example: <br> To populate the value of response attribute uid under name CUSTOM-USER-NAME: enter
 uid in Map Key field, and enter CUSTOM-USER-NAME in Corresponding Map Value field.",
          "propertyOrder" : 9200,
          "patternProperties" : {
            ".*" : {
              "type" : "string"
            }
```

```
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "object",
              "required" : false
            }
          }
        },
        "continuousSecurityHeaders" : {
          "title" : "Continuous Security Headers",
          "description" : "The name of the headers in the user's original request, that will be sent
 as part of the payload during policy evaluation, which can then be accessed via the 'environment'
 variable in a policy script. The 'key' is the name of the header to be sent, and the 'value' is the
 name which it will appear as in the policy evaluation script.It is possible to map multiple headers
 to the same name (they will simply appear as an array in the evaluation script). If the header
 doesn't exist, then the empty string will be sent.",
          "propertyOrder" : 3211,
          "patternProperties" : {
            ".*" : {
              "type" : "string"
            }
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "object",
              "required" : false
            }
          }
        },
        "loginFormUri" : {
          "title" : "Login Form URI",
          "description" : "List of absolute URIs corresponding to an application's web.xml form-login-
page element. (property name: com.sun.identity.agents.config.login.form)  <br> Example: <br> /BankApp/
jsp/login.jsp",
          "propertyOrder" : 2800,
          "items" : {
            "type" : "string"
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "array",
```

```
              "required" : false
            }
          }
        },
        "notEnforcedUrisCacheSize" : {
          "title" : "Not Enforced URIs Cache Size",
          "description" : "Size of the cache to be used if caching of not enforced URI list evaluation
results is enabled. (property name: org.forgerock.agents.notenforced.uri.cache.size) ",
          "propertyOrder" : 7800,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "integer",
              "required" : false
            }
          }
        },
        "notEnforcedUrisCacheEnabled" : {
          "title" : "Not Enforced URIs Cache Enabled",
          "description" : "Enables the caching of the Not Enforced URIs list evaluation results.
(property name: org.forgerock.agents.notenforced.uri.cache.enabled) ",
          "propertyOrder" : 7700,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : false
            }
          }
        },
        "sessionAttributeMap" : {
          "title" : "Session Attribute Mapping",
          "description" : "Maps the session attributes to be populated under specific names for the
currently authenticated user. (property name: org.forgerock.agents.session.attribute.map)   <br>
Example: <br>  To populate the value of session attribute UserToken under name CUSTOM-userid: enter
UserToken in Map Key field, and enter CUSTOM-userid in Corresponding Map Value field.",
          "propertyOrder" : 9000,
          "patternProperties" : {
            ".*" : {
              "type" : "string"
            }
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
```

```
            "value" : {
              "type" : "object",
              "required" : false
            }
          }
        },
        "invertNotEnforcedUris" : {
          "title" : "Invert Not Enforced URIs",
          "description" : "Inverts protection of  URIs specified in Not Enforced URIs list. When set
to true, it indicates that the URIs specified should be enforced and all other URIs should be not
enforced by the Agent. (property name: org.forgerock.agents.notenforced.uri.invert.enabled) ",
          "propertyOrder" : 7600,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : false
            }
          }
        },
        "logoutIntrospection" : {
          "title" : "Logout Introspect Enabled",
          "description" : "Allows the Agent to search HTTP request body to locate logout parameter.
(property name: org.forgerock.agents.logout.introspection.enabled) ",
          "propertyOrder" : 6200,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : false
            }
          }
        }
      }
    },
    "globalJ2EEAgentConfig" : {
      "type" : "object",
      "title" : "Global",
      "propertyOrder" : 0,
      "properties" : {
        "fqdnMapping" : {
          "title" : "FQDN Virtual Host Map",
          "description" : "Maps virtual, invalid, or partial hostnames, and IP addresses to the
FQDN to access protected resources. (property name: org.forgerock.agents.fqdn.map)  <br> Examples:
<br>  To map the partial hostname myserver to myserver.mydomain.com: enter myserver in the Map
Key field and myserver.mydomain.com in the Corresponding Map Value field. To map a virtual server
rst.hostname.com that points to the actual server abc.hostname.com: enter valid1 in the Map Key field
and rst.hostname.com in the Corresponding Map Value field.",
          "propertyOrder" : 6600,
```

```
          "patternProperties" : {
            ".*" : {
              "type" : "string"
            }
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "object",
              "required" : false
            }
          }
        },
        "localAuditRotationSize" : {
          "title" : "Local Audit Log Rotation Size",
          "description" : "Size limit when a local audit log file is rotated to a new file. (property
name: com.sun.identity.agents.config.local.log.size) ",
          "propertyOrder" : 1900,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "integer",
              "required" : false
            }
          }
        },
        "agentSessionChangeNotificationsEnabled" : {
          "title" : "Session Logout Notification ",
          "description" : "Flag to indicate whether the Agent will subscribe
to session logout notifications (via websockets) from AM. (property:
org.forgerock.agents.session.change.notifications.enabled)",
          "propertyOrder" : 12110,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : false
            }
          }
        },
        "localAuditLogRotation" : {
          "title" : "Rotate Local Audit Log",
          "description" : "Flag to indicate that audit log files should be rotated when reaching a
certain size. (property name: org.forgerock.agents.local.audit.log.rotation.enabled) ",
```

```
          "propertyOrder" : 1800,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : false
            }
          }
        },
        "redirectAttemptLimitCookieName" : {
          "title" : "Redirect Attempt Cookie Name",
          "description" : "Agent tries to detect redirect loops while authenticating, which would
normally indicate a cookie domain problem.  The Agent does this by using a cookie to holds the
current redirection count. (property: org.forgerock.agents.redirect.cookie.name)",
          "propertyOrder" : 7150,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "configurationReloadInterval" : {
          "title" : "Configuration Reload Interval",
          "description" : "Only used when websocket notifications are disabled, specifies
interval in seconds after which config is reloaded automatically by the Agent. (property name:
org.forgerock.agents.config.reload.seconds) ",
          "propertyOrder" : 1200,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "integer",
              "required" : false
            }
          }
        },
        "debugLogfileRotationMinutes" : {
          "title" : "Debug File Rotation Time",
          "description" : "This is the time in minutes after which log file rotation will occur.
(property: org.forgerock.agents.debug.rotation.time.minutes)",
          "propertyOrder" : 10040,
          "type" : "object",
          "exampleValue" : "",
```

```
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "integer",
              "required" : false
            }
          }
        },
        "agentConfigChangeNotificationsEnabled" : {
          "title" : "Agent Configuration Change Notification",
          "description" : "Enable agent to receive notification messages
(via websockets) from AM server for configuration changes. (property name:
org.forgerock.agents.config.change.notifications.enabled) ",
          "propertyOrder" : 12100,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : false
            }
          }
        },
        "customResponseHeader" : {
          "title" : "Custom Response Header",
          "description" : "Map specifies the custom headers that are set by the Agent on the client
browser. The key is the header name and the value represents the header value. (property name:
org.forgerock.agents.response.header.map)  <br> Example: <br>  To set the custom header Cache-Control
to value no-cache: enter Cache-Control in Map Key field, and enter no-cache in Corresponding Map
Value field.",
          "propertyOrder" : 7000,
          "patternProperties" : {
            ".*" : {
              "type" : "string"
            }
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "object",
              "required" : false
            }
          }
        },
        "debugLevel" : {
          "title" : "Agent Debug Level",
```

```
          "description" : "Specifies type of agent debug messages to log. (property name:
com.iplanet.services.debug.level) ",
          "propertyOrder" : 10000,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "preAuthCookieMaxAge" : {
          "title" : "Pre-Authenticated Cookie Max Age",
          "description" : "This is the amount of time in seconds before the pre-authn cookie will
timeout. (property: org.forgerock.agents.authn.cookie.max.age.seconds)",
          "propertyOrder" : 11220,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "integer",
              "required" : false
            }
          }
        },
        "debugLogfileRetentionCount" : {
          "title" : "Debug File Rotation Retention Count",
          "description" : "This is the number of log files to retain after rotation, so for example,
setting it to 10 would give you one current debug file and nine older (rotated) files. (property:
org.forgerock.agents.debug.retention.count)",
          "propertyOrder" : 10050,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "integer",
              "required" : false
            }
          }
        },
        "fqdnCheck" : {
          "title" : "FQDN Check",
          "description" : "Enables checking of fqdn default value and fqdn map values. (property name:
org.forgerock.agents.fqdn.check.enabled) ",
          "propertyOrder" : 6400,
          "type" : "object",
```

```
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : false
            }
          }
        },
        "webSocketConnectionIntervalInMinutes" : {
          "title" : "Web Socket Connection Interval",
          "description" : "Interval in minutes by which agents reopen their web socket
connection to ensure a fair distribution of connections across AM servers. (property:
org.forgerock.agents.balance.websocket.interval.minutes).",
          "propertyOrder" : 12120,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "integer",
              "required" : false
            }
          }
        },
        "preAuthCookieName" : {
          "title" : "Pre-Authenticated Cookie Name",
          "description" : "Specifies the name of the cookie the agent uses to track the progress of
authentication with AM. (property: org.forgerock.agents.authn.cookie.name)",
          "propertyOrder" : 11210,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "httpSessionBinding" : {
          "title" : "HTTP Session Binding",
          "description" : "If true will invalidate the http session when login has failed,
user has no SSO session, or principal user name does not match SSO user name. (property name:
org.forgerock.agents.http.session.binding.enabled) ",
          "propertyOrder" : 3500,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
```

```
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : false
            }
          }
        },
        "userTokenName" : {
          "title" : "User Token Name",
          "description" : "Session property name for user-ID of the authenticated user in session.
(property name: org.forgerock.agents.userid.mapping.mode.use.session.property.name) ",
          "propertyOrder" : 900,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "userpassword" : {
          "title" : "Password",
          "description" : "",
          "propertyOrder" : 100,
          "required" : true,
          "type" : "string",
          "format" : "password",
          "exampleValue" : ""
        },
        "auditAccessType" : {
          "title" : "Audit Access Types",
          "description" : "Types of messages to log based on user URL access attempts. (property name:
org.forgerock.agents.audit.what) ",
          "propertyOrder" : 1500,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "userMappingMode" : {
          "title" : "User Mapping Mode",
          "description" : "Specifies mechanism agent uses to determine user-ID. (property name:
org.forgerock.agents.user.mapping.mode) ",
          "propertyOrder" : 600,
```

```
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "repositoryLocation" : {
          "title" : "Location of Agent Configuration Repository",
          "description" : "Indicates agent's configuration located either on agent's host or centrally
on AM server (property: org.forgerock.agents.config.location).",
          "propertyOrder" : 400,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "status" : {
          "title" : "Status",
          "description" : "Status of the agent configuration.",
          "propertyOrder" : 200,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : true
            }
          }
        },
        "localAuditLogfileRetentionCount" : {
          "title" : "Audit Logfile Retention Count",
          "description" : "The number of audit log files to retain after rotation has occurred.
(property: org.forgerock.agents.local.audit.log.retention.count)",
          "propertyOrder" : 2100,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "integer",
              "required" : false
            }
          }
        },
        "fqdnDefault" : {
          "title" : "FQDN Default",
```

```
          "description" : "Fully qualified hostname that the users should use in order to access
resources. (property name: org.forgerock.agents.fqdn.default) ",
          "propertyOrder" : 6500,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "loginAttemptLimitCookieName" : {
          "title" : "Login Attempt Limit Cookie Name",
          "description" : "The name of the cookie used to record the number of login attempts.
(property: org.forgerock.agents.login.counter.cookie.name)",
          "propertyOrder" : 4500,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "jwtName" : {
          "title" : "JWT Cookie Name",
          "description" : "The name used by the agent to set the OIDC JWT on the user's browser.
(property: org.forgerock.agents.jwt.cookie.name)",
          "propertyOrder" : 11201,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "redirectAttemptLimit" : {
          "title" : "Redirect Attempt Limit",
          "description" : "Number of successive single point redirects that a user can make using a
single browser session which will trigger the blocking of the user request. Set to 0 to disable this
feature. (property name: org.forgerock.agents.redirect.attempt.limit) ",
          "propertyOrder" : 7100,
          "type" : "object",
```

```
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "integer",
              "required" : false
            }
          }
        },
        "agentgroup" : {
          "title" : "Group",
          "description" : "Add the agent to a group to allow inheritance of property values from the
group. <br>Changing the group will update inherited property values. <br>Inherited property values
are copied to the agent.",
          "propertyOrder" : 50,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "userAttributeName" : {
          "title" : "User Attribute Name",
          "description" : "Name of the attribute which contains the user-ID. (property name:
org.forgerock.agents.user.mapping.mode.attribute.name) ",
          "propertyOrder" : 700,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "debugLogfileDirectory" : {
          "title" : "Debug Logfile Directory",
          "description" : "Location of the agent logs files, and where monitoring CSV files are
written. This is normally set in bootstrap properties during the install process. Note there is no
default and no logging will occur until a value for this property is provided. Anything logged will
be written to the standard output and may end up in the container log file (so \"catalina.out\" in
the case of Tomcat). (property: org.forgerock.agents.csv.monitoring.directory)",
          "propertyOrder" : 10060,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
```

```
        }
      },
      "debugLogfilePrefix" : {
        "title" : "Debug File Rotation Prefix",
        "description" : "Prefix which can be added onto the front of the debug file name when it is
rotated. (property: org.forgerock.agents.debug.prefix)",
        "propertyOrder" : 10010,
        "type" : "object",
        "exampleValue" : "",
        "properties" : {
          "inherited" : {
            "type" : "boolean",
            "required" : true
          },
          "value" : {
            "type" : "string",
            "required" : false
          }
        }
      },
      "localAuditLogfilePath" : {
        "title" : "Audit Logfile Path",
        "description" : "The full path of the local auditing file. (property:
org.forgerock.agents.local.audit.file.path)",
        "propertyOrder" : 2000,
        "type" : "object",
        "exampleValue" : "",
        "properties" : {
          "inherited" : {
            "type" : "boolean",
            "required" : true
          },
          "value" : {
            "type" : "string",
            "required" : false
          }
        }
      },
      "cdssoRootUrl" : {
        "title" : "Agent Root URL for CDSSO",
        "description" : "The agent root URL for CDSSO. The valid value is in the following format:
<br>protocol://hostname:port/<br> The protocol represents the protocol used, such as http or https.
The hostname represents the host name of the machine on which the agent resides. The port represents
the port number on which the agent is installed. The slash following the port number is required.",
        "propertyOrder" : 22700,
        "items" : {
          "type" : "string"
        },
        "type" : "object",
        "exampleValue" : "",
        "properties" : {
          "inherited" : {
            "type" : "boolean",
            "required" : true
          },
          "value" : {
            "type" : "array",
            "required" : false
          }
```

```
        }
      },
      "filterMode" : {
        "title" : "Agent Filter Mode",
        "description" : "Specifies the mode of operation of the Filter. (property name:
org.forgerock.agents.filter.mode.map) <br>Valid key: the web application name. <br>Valid values:
ALL, URL_POLICY, SSO_ONLY, NONE <br>For this property, a global value can be set to apply to all
the applications that don't have their own specific filter mode. <br>Examples: <br>To set ALL as the
global filter mode: leave Map Key field empty, and enter ALL in Corresponding Map Value field. <br>To
set URL_POLICY as the filter mode for application BankApp: enter BankApp in Map Key field, and enter
URL_POLICY in Corresponding Map Value field.",
        "propertyOrder" : 500,
        "patternProperties" : {
          ".*" : {
            "type" : "string"
          }
        },
        "type" : "object",
        "exampleValue" : "",
        "properties" : {
          "inherited" : {
            "type" : "boolean",
            "required" : true
          },
          "value" : {
            "type" : "object",
            "required" : false
          }
        }
      },
      "loginAttemptLimit" : {
        "title" : "Login Attempt Limit",
        "description" : "Limit of failed login attempts for a user's single browser session until
triggering the blocking of the user request. Value of 0 disables this feature. (property name:
org.forgerock.agents.login.attempt.limit.count) ",
        "propertyOrder" : 4400,
        "type" : "object",
        "exampleValue" : "",
        "properties" : {
          "inherited" : {
            "type" : "boolean",
            "required" : true
          },
          "value" : {
            "type" : "integer",
            "required" : false
          }
        }
      },
      "debugLogfileRotationSize" : {
        "title" : "Debug File Rotation Size",
        "description" : "This specifies the approximate size in bytes at which a log file will be
rotated to a new log file. (property: org.forgerock.agents.debug.rotation.size.bytes)",
        "propertyOrder" : 10030,
        "type" : "object",
        "exampleValue" : "",
        "properties" : {
          "inherited" : {
            "type" : "boolean",
```

```
              "required" : true
            },
            "value" : {
              "type" : "integer",
              "required" : false
            }
          }
        },
        "fallforwardModeEnabled" : {
          "title" : "Fall-Forward Mode",
          "description" : "This property is used when AM is not available. <br>  Disabled: the
Agent will deny every incoming request with an HTTP 403 <br>  Enabled: the Agent will continue
to allow access to any resource matched by a not enforced rule until AM becomes available again
<br><br>(property: org.forgerock.agents.session.change.notifications.enabled) (Agent 5.7+ only)",
          "propertyOrder" : 12115,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : false
            }
          }
        },
        "userPrincipalFlag" : {
          "title" : "User Principal Flag",
          "description" : "Use principal instead of just the user-ID for authenticating the user.
(property name: org.forgerock.agents.userid.mapping.mode.use.dn.enabled) ",
          "propertyOrder" : 800,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : false
            }
          }
        },
        "debugLogfileSuffix" : {
          "title" : "Debug File Rotation Suffix",
          "description" : "This is a value appended onto the end of the debug file name when it is
rotated. The user is free to define it as they want, but if it does not involve a timestamp that
produces different file names when the rotation time is reached, log file rotation is unlikely to
function correctly (property: org.forgerock.agents.debug.suffix)",
          "propertyOrder" : 10020,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
```

```
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "auditLogLocation" : {
          "title" : "Audit Log Location",
          "description" : "LOCAL = audit information stored in files based locally
to the Agent container <br>REMOTE = audit information logged via AM. (property name:
org.forgerock.agents.audit.where) ",
          "propertyOrder" : 1600,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        }
      }
    },
    "amServicesJ2EEAgent" : {
      "type" : "object",
      "title" : "AM Services",
      "propertyOrder" : 3,
      "properties" : {
        "urlPolicyEnvJsessionParameters" : {
          "title" : "URL Policy Env jsession Parameters",
          "description" : "List of HTTP SESSION attributes whose names and values will
be set in the environment map for URL policy evaluation at AM server. (property name:
org.forgerock.agents.continuous.security.http.session.list)  <br> Examples: <br> name <br>
phonenumber",
          "propertyOrder" : 12000,
          "items" : {
            "type" : "string"
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "array",
              "required" : false
            }
          }
        },
        "conditionalLoginUrl" : {
          "title" : "AM Conditional Login URL",
```

```
          "description" : "(property name: org.forgerock.openam.agents.config.conditional.login.url)
  <br> Examples: <br> match|url?param1=value1&amp;ampparam2=value2 <br> match/path|?
param1=value1&amp;ampparam2=value2&amp;ampparam3=value3",
          "propertyOrder" : 3800,
          "items" : {
            "type" : "string"
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "array",
              "required" : false
            }
          }
        },
        "authSuccessRedirectUrl" : {
          "title" : "Redirect to AM's Success URL",
          "description" : "When enabled, the Agent will redirect to the session's Success URL instead
 (defined in auth. chain) of the originally requested resource after successful authentication.
 (property: org.forgerock.agents.authn.success.redirect.session.url.enabled)",
          "propertyOrder" : 4000,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : false
            }
          }
        },
        "agentAdviceEncode" : {
          "title" : "Composite Advice Encode",
          "description" : "This property is used to specify whether AM composite advices
 should be based64url encoded before sending to custom login endpoints. (property:
 org.forgerock.agents.advice.b64.url.encode)",
          "propertyOrder" : 13050,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : false
            }
          }
        },
        "policyEvaluationRealm" : {
```

```
          "title" : "Policy Evaluation Realm",
          "description" : "Which realm to start evaluating from. (property name:
org.forgerock.agents.policy.evaluation.realm.map) ",
          "propertyOrder" : 5400,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "authServicePort" : {
          "title" : "AM Authentication Service Port",
          "description" : "Port to be used by the AM authentication service. This property need
to be updated in OpenSSOAgentBootstrap.properties (property name: org.forgerock.agents.am.port)
<br>Required Agent Restart",
          "propertyOrder" : 11100,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "integer",
              "required" : false
            }
          }
        },
        "customLoginEnabled" : {
          "title" : "Allow Custom Login Mode",
          "description" : "Flag to enable custom login. (property:
org.forgerock.agents.legacy.login.enabled)",
          "propertyOrder" : 3700,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : false
            }
          }
        },
        "urlPolicyEnvPostParameters" : {
          "title" : "URL Policy Env POST Parameters",
          "description" : "List of HTTP POST request parameters whose names and values
will be set in the environment map for URL policy evaluation at AM server. (property name:
org.forgerock.agents.continuous.security.post.list)  <br> Examples: <br> name <br> phonenumber",
```

```
          "propertyOrder" : 11900,
          "items" : {
            "type" : "string"
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "array",
              "required" : false
            }
          }
        },
        "policyEvaluationApplication" : {
          "title" : "Policy Set",
          "description" : "Which application contains the policies to evaluate with. (property name:
org.forgerock.agents.policy.set.map) ",
          "propertyOrder" : 5500,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "urlPolicyEnvGetParameters" : {
          "title" : "URL Policy Env GET Parameters",
          "description" : "List of HTTP GET request parameters whose names and values will
be set in the environment map for URL policy evaluation at AM server. (property name:
org.forgerock.agents.continuous.security.get.list)  <br> Examples: <br> name <br> phonenumber",
          "propertyOrder" : 11800,
          "items" : {
            "type" : "string"
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "array",
              "required" : false
            }
          }
        },
        "legacyLoginUrlList" : {
          "title" : "Custom Conditional Login URL",
```

```
          "description" : "Conditionally redirect users based on the incoming request URL.
 If the incoming request URL matches a specified domain name, the Java agent redirects
 the request to a specific URL. Conditional redirects have the format [Domain/path]|
[URL?realm=value&amp;parameter1=value1...], with no spaces between values. <br>Example:
 myapp.domain.com|https://login.example.com/apps/login.jsp?realm=sales  <br>(property:
 org.forgerock.openam.agents.config.conditional.custom.login.url)",
          "propertyOrder" : 3900,
          "items" : {
            "type" : "string"
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "array",
              "required" : false
            }
          }
        },
        "authServiceProtocol" : {
          "title" : "AM Authentication Service Protocol",
          "description" : "Protocol to be used by the AM authentication service. This property need
 to be updated in OpenSSOAgentBootstrap.properties (property name: org.forgerock.agents.am.protocol)
 <br>Required Agent Restart",
          "propertyOrder" : 10900,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "policyNotifications" : {
          "title" : "Enable Policy Notifications",
          "description" : "Enable Notifications(via websockets) for remote policy client. (property
 name: org.forgerock.agents.policy.change.notifications.enabled) <br>Required Agent Restart",
          "propertyOrder" : 11200,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : false
            }
          }
```

```
      },
      "amLoginUrl" : {
        "title" : "AM Login URL",
        "description" : "AM login page URL. (property name:
com.sun.identity.agents.config.login.url)  <br> Example: <br> http://host:port/am/UI/Login",
        "propertyOrder" : 3710,
        "items" : {
          "type" : "string"
        },
        "type" : "object",
        "exampleValue" : "",
        "properties" : {
          "inherited" : {
            "type" : "boolean",
            "required" : true
          },
          "value" : {
            "type" : "array",
            "required" : false
          }
        }
      },
      "restrictToRealm" : {
        "title" : "Restrict To Realm",
        "description" : "A map keyed by application name which allows users from only the
specified realms (each entry is a CSV) to access the specified application. If no restricted
realm is set, any user from any realm will be allowed access. Keyed by application name,
value is a comma separated list of realms from which users may request resources. (property:
org.forgerock.agents.restrict.to.realm.map)",
        "propertyOrder" : 13080,
        "patternProperties" : {
          ".*" : {
            "type" : "string"
          }
        },
        "type" : "object",
        "exampleValue" : "",
        "properties" : {
          "inherited" : {
            "type" : "boolean",
            "required" : true
          },
          "value" : {
            "type" : "object",
            "required" : false
          }
        }
      },
      "authServiceHost" : {
        "title" : "AM Authentication Service Host Name",
        "description" : "Host name to be used by the AM authentication service. This property need
to be updated in OpenSSOAgentBootstrap.properties (property name: org.forgerock.agents.am.hostname)
<br>Required Agent Restart",
        "propertyOrder" : 11000,
        "type" : "object",
        "exampleValue" : "",
        "properties" : {
          "inherited" : {
            "type" : "boolean",
```

```
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "conditionalLogoutUrl" : {
          "title" : "AM Conditional Logout URL",
          "description" : "(property name: org.forgerock.agents.conditional.logout.url.list)
  <br> Examples: <br> match|url?param1=value1&amp;param2=value2 <br> match/path|?
param1=value1&amp;param2=value2&amp;param3=value3",
          "propertyOrder" : 12550,
          "items" : {
            "type" : "string"
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "array",
              "required" : false
            }
          }
        }
      }
    }
  }
}
```

delete

Usage:

```
am> delete J2eeAgents --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action J2eeAgents --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action J2eeAgents --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action J2eeAgents --realm Realm --actionName nextdescendents
```

query

Querying the agents of a specific type

Usage:

```
am> query J2eeAgents --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read J2eeAgents --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update J2eeAgents --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "ssoJ2EEAgentConfig" : {
      "type" : "object",
      "title" : "SSO",
      "propertyOrder" : 2,
      "properties" : {
        "cookieResetPaths" : {
          "title" : "Cookies Reset Path Map",
          "description" : "Maps cookie names specified in Cookie Reset Name List to value
being the path of this cookie to be used when a reset event occurs. (property name:
org.forgerock.agents.cookie.reset.path.map) ",
          "propertyOrder" : 4900,
          "patternProperties" : {
            ".*" : {
              "type" : "string"
            }
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "object",
              "required" : false
            }
          }
        },
        "setCookieAttributeMap" : {
          "title" : "Set-Cookie Attribute Map",
          "description" : "Text from this map will be added directly into the Set-Cookie header
by the AttributeTaskHandler and its decendents when it creates cookies out of Profile Attributes,
Session Info Attributes and/or Response Attributes. The key is the cookie name, the value is any
arbitrary text suitable for the Set-Cookie header. Users should remember semicolons if they wish
to add multiple values.  Values inappropriate for the header will likely cause the Agent to fail to
create the relevant cookie. (property: org.forgerock.agents.set.cookie.attribute.map)",
          "propertyOrder" : 5950,
          "patternProperties" : {
            ".*" : {
              "type" : "string"
            }
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
```

```
            "required" : true
          },
          "value" : {
            "type" : "object",
            "required" : false
          }
        }
      },
      "acceptIPDPCookie" : {
        "title" : "Convert SSO Tokens into OpenID Connect JWTs",
        "description" : "When this property is set to true, for each incoming request, when the
user does not present a JWT in the designated cookie, the Agent will look for an SSO token in the
iPlanetDirectoryPro cookie (configurable in AM). If this is found, the Agent invokes AM to exchange
it for a JWT which is then used in further requests. The result is cached, so interaction with AM
will not be needed, if the same SSO token is presented in the future (and the existing cache entry is
still valid) (property: org.forgerock.agents.accept.ipdp.cookie.enabled)",
        "propertyOrder" : 5900,
        "type" : "object",
        "exampleValue" : "",
        "properties" : {
          "inherited" : {
            "type" : "boolean",
            "required" : true
          },
          "value" : {
            "type" : "boolean",
            "required" : false
          }
        }
      },
      "httpOnly" : {
        "title" : "Http Only",
        "description" : "Flag saying whether HTTP only cookies are enabled. (property:
com.sun.identity.cookie.httponly)",
        "propertyOrder" : 5910,
        "type" : "object",
        "exampleValue" : "",
        "properties" : {
          "inherited" : {
            "type" : "boolean",
            "required" : true
          },
          "value" : {
            "type" : "boolean",
            "required" : false
          }
        }
      },
      "authExchangeCookieName" : {
        "title" : "Authentication Exchange Cookie Name",
        "description" : "This property allows the administrator to define a cooke name that will be
used by the authn exchange endpoint. The value is empty by default and the endpoint will thus not be
capable of examining cookie values (property: org.forgerock.agents.authn.exchange.cookie.name) (Agent
5.7+ only)",
        "propertyOrder" : 5902,
        "type" : "object",
        "exampleValue" : "",
        "properties" : {
          "inherited" : {
```

```
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "cdssoRedirectUri" : {
          "title" : "CDSSO Redirect URI",
          "description" : "An intermediate URI that is used by the Agent for processing CDSSO
requests. (property name: org.forgerock.agents.authn.redirect.uri) ",
          "propertyOrder" : 5100,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "cookieResetDomains" : {
          "title" : "Cookies Reset Domain Map",
          "description" : "Maps cookie names specified in Cookie Reset Name List to value
being the domain of this cookie to be used when a reset event occurs. (property name:
org.forgerock.agents.cookie.reset.domain.map) ",
          "propertyOrder" : 4800,
          "patternProperties" : {
            ".*" : {
              "type" : "string"
            }
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "object",
              "required" : false
            }
          }
        },
        "cdssoSecureCookies" : {
          "title" : "CDSSO Secure Enable",
          "description" : "The SSO Token cookie set by the agent in the different domains in CDSSO
mode will be marked secure. Only transmitted if the communications channel with host is a secure one.
(property name: org.forgerock.agents.secure.cookies.enabled) ",
          "propertyOrder" : 5700,
          "type" : "object",
          "exampleValue" : "",
```

```
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : false
            }
          }
        },
        "authExchangeUri" : {
          "title" : "Authentication Exchange URI",
          "description" : "This property allows the administrator to enable an endpoint that will
facilitate the exchange of SSO tokens for OIDC JWTs. The value is empty by default and thus the
endpoint is not accessible. (property: org.forgerock.agents.authn.exchange.uri) (Agent 5.7+ only)",
          "propertyOrder" : 5901,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "setCookieInternalMap" : {
          "title" : "Set-Cookie Internal Map",
          "description" : "Text from this map will be added directly into the Set-Cookie header
when creating \"internal\" cookies (e.g. the am-auth-jwt and pre-auth cookies). This allows, among
other things, the same-site value to be manipulated. The key is the cookie name, the value is any
arbitrary text suitable for the Set-Cookie header. Users should remember semicolons if they wish
to add multiple values.  Values inappropriate for the header will likely cause the Agent to fail to
create the relevant cookie. (property: org.forgerock.agents.set.cookie.internal.map)",
          "propertyOrder" : 5940,
          "patternProperties" : {
            ".*" : {
              "type" : "string"
            }
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "object",
              "required" : false
            }
          }
        },
        "secureCookies" : {
          "title" : "Secure Cookies",
```

```
          "description" : "On setting this property to true, all cookies created by the
Agent will be secure. The value is set to false for backwards compatibility. (property:
org.forgerock.agents.jwt.cookie.secure.enabled)",
          "propertyOrder" : 5930,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : false
            }
          }
        },
        "cookieResetEnabled" : {
          "title" : "Cookie Reset",
          "description" : "Agent resets cookies in the response before redirecting to authentication.
(property name: org.forgerock.agents.cookie.reset.enabled) ",
          "propertyOrder" : 4600,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : false
            }
          }
        },
        "cdssoDomainList" : {
          "title" : "CDSSO Domain List",
          "description" : "Domains for which cookies have to be set in a CDSSO scenario. (property
name: org.forgerock.agents.jwt.cookie.domain.list)  <br> Example: <br> .sun.com",
          "propertyOrder" : 5800,
          "items" : {
            "type" : "string"
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "array",
              "required" : false
            }
          }
        },
        "cookieResetNames" : {
          "title" : "Cookies Reset Name List",
```

```
          "description" : "Cookie names that will be reset by the Agent if Cookie Reset is enabled.
(property name: org.forgerock.agents.cookie.reset.name.list) ",
          "propertyOrder" : 4700,
          "items" : {
            "type" : "string"
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "array",
              "required" : false
            }
          }
        },
        "excludedUserAgentsList" : {
          "title" : "Samesite Cookie Attributes Excluded User Agents Pattern List",
          "description" : "Excluded User agents pattern list. List of incompatible
user agents that will be prevented from receiving SameSite cookie attributes. <br>
(Property:org.forgerock.agents.samesite.excluded.user.agents.list)",
          "propertyOrder" : 5960,
          "items" : {
            "type" : "string"
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "array",
              "required" : false
            }
          }
        },
        "encodeCookies" : {
          "title" : "Encode Cookies",
          "description" : "Cookies are encoded, if set. (property: com.iplanet.am.cookie.encode)",
          "propertyOrder" : 5920,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : false
            }
          }
        }
      }
```

```
   },
   "advancedJ2EEAgentConfig" : {
     "type" : "object",
     "title" : "Advanced",
     "propertyOrder" : 5,
     "properties" : {
       "postDataStickySessionMode" : {
         "title" : "PDP Stickysession mode",
         "description" : "If the PDP mechanism needs sticky loadbalancing, the URL mode
will append a querystring, while the Cookie mode will create a cookie. (property name:
org.forgerock.agents.pdp.sticky.session.mode)",
         "propertyOrder" : 13400,
         "type" : "object",
         "exampleValue" : "",
         "properties" : {
           "inherited" : {
             "type" : "boolean",
             "required" : true
           },
           "value" : {
             "type" : "string",
             "required" : false
           }
         }
       },
       "alternativeAgentHostname" : {
         "title" : "Alternative Agent Host Name",
         "description" : "Host name identifying the Agent protected server to the client browsers if
different from the actual host name. (property name: org.forgerock.agents.agent.hostname) ",
         "propertyOrder" : 4100,
         "type" : "object",
         "exampleValue" : "",
         "properties" : {
           "inherited" : {
             "type" : "boolean",
             "required" : true
           },
           "value" : {
             "type" : "string",
             "required" : false
           }
         }
       },
       "postDataCacheTtlMin" : {
         "title" : "PDP Cache TTL in Minutes",
         "description" : "This sets the time in minutes after which entries in the Post Data
Preservation cache will timeout and be purged. (property: org.forgerock.agents.pdp.cache.ttl.minutes)
<br>Required Agent Restart",
         "propertyOrder" : 13300,
         "type" : "object",
         "exampleValue" : "",
         "properties" : {
           "inherited" : {
             "type" : "boolean",
             "required" : true
           },
           "value" : {
             "type" : "integer",
             "required" : false
```

```
            }
          }
        },
        "ssoExchangeCacheTTL" : {
          "title" : "Exchanged SSO Token Cache Time to Live",
          "description" : "This sets the time in minutes after which entries in the SSO token
exchange cache will timeout and be purged.  Since exchanging SSO tokens for JWTs is an expensive
process, previously exchanged SSO tokens are cached so that the roundtrip to AM can be avoided
in the case where an entity is unable to permanently store its JWT in a cookie. (property:
org.forgerock.agents.sso.exchange.cache.ttl.minutes) <br>Required Agent Restart",
          "propertyOrder" : 13900,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "integer",
              "required" : false
            }
          }
        },
        "clientHostnameHeader" : {
          "title" : "Client Hostname Header",
          "description" : "HTTP header name that holds the Hostname of the client. (property name:
org.forgerock.agents.http.header.containing.remote.hostname) ",
          "propertyOrder" : 1100,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "xssDetectionRedirectUri" : {
          "title" : "XSS detection redirect URI",
          "description" : "An application-specific Map that identifies a URI of the customized page if
XSS code has been deteced. (property name: org.forgerock.agents.xss.redirect.uri.map)  <br>Examples:
<br>To set a redirect target for application BankApp: enter BankApp in Map Key field, and enter a
redirect URI in Corresponding Map Value field.",
          "propertyOrder" : 12900,
          "patternProperties" : {
            ".*" : {
              "type" : "string"
            }
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
```

```
              "required" : true
            },
            "value" : {
              "type" : "object",
              "required" : false
            }
          }
        },
        "ssoExchangeCacheSize" : {
          "title" : "Exchanged SSO Token Cache Size",
          "description" : "The number of entries in the SSO Exchange cache. (property:
org.forgerock.agents.sso.exchange.cache.size) <br>Required Agent Restart",
          "propertyOrder" : 13910,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "integer",
              "required" : false
            }
          }
        },
        "customProperties" : {
          "title" : "Custom Properties",
          "description" : "Additional properties that allow users to augment the set of
properties supported by agent. (property name: com.sun.identity.agents.config.freeformproperties)
 <br> Examples: <br> customproperty=custom-value1 <br> customlist[0]=customlist-value-0
<br> customlist[1]=customlist-value-1 <br> custommap[key1]=custommap-value-1 <br>
custommap[key2]=custommap-value-2",
          "propertyOrder" : 20000,
          "items" : {
            "type" : "string"
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "array",
              "required" : false
            }
          }
        },
        "postDataPreserveCacheEntryMaxEntries" : {
          "title" : "PDP Maximum Number of Cache Entries",
          "description" : "Maximum number of entries to hold in the PDP cache (Property name:
org.forgerock.agents.pdp.cache.size).",
          "propertyOrder" : 13550,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
```

```
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "integer",
              "required" : false
            }
          }
        },
        "postDataPreservation" : {
          "title" : "Post Data Preservation enabled",
          "description" : "Post Data Preservation functionality basically stores any POST
data before redirecting the user to the login screen and after successful login the agent
will generate a page that autosubmits the same POST to the original URL. (property name:
org.forgerock.agents.post.data.preservation.enabled)",
          "propertyOrder" : 13100,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : false
            }
          }
        },
        "monitoringToCSV" : {
          "title" : "Export Monitoring Metrics to CSV",
          "description" : "When set to true, the Agent will write monitoring information to CSV files.
(property: org.forgerock.agents.monitoring.to.csv.enabled)",
          "propertyOrder" : 13085,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : false
            }
          }
        },
        "idleTimeRefreshWindow" : {
          "title" : "Idle Time Refresh Window",
          "description" : "Once every this number of minutes, the Agent will nudge AM so
it knows a particular session is still in use, thereby resetting its idle time. (property:
org.forgerock.agents.idle.time.window.minutes)",
          "propertyOrder" : 14200,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
```

```
            },
            "value" : {
              "type" : "integer",
              "required" : false
            }
          }
        },
        "clientIpHeader" : {
          "title" : "Client IP Address Header",
          "description" : "HTTP header name that holds the IP address of the client. (property name:
org.forgerock.agents.http.header.containing.ip.address) ",
          "propertyOrder" : 1000,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "policyCachePerUser" : {
          "title" : "Policy Cache Per User",
          "description" : "This is the number of distinct policy evaluation entries that each session
(stored in the policy evaluation cache) can have.  Thus the total number of policy evaluation
results that can be stored is the \"Policy Cache Size\" multiplied by the \"Policy Cache Per User\".
(property: org.forgerock.agents.policy.cache.per.session.size) <br>Required Agent Restart",
          "propertyOrder" : 14100,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "integer",
              "required" : false
            }
          }
        },
        "alternativeAgentPort" : {
          "title" : "Alternative Agent Port Number",
          "description" : "Port number identifying the Agent protected server listening
port to the client browsers if different from the actual listening port. (property name:
org.forgerock.agents.agent.port) ",
          "propertyOrder" : 4200,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
```

```
              "type" : "string",
              "required" : false
            }
          }
        },
        "postDataPreserveCacheEntryMaxTotalSizeMb" : {
          "title" : "PDP Maximum Cache Size",
          "description" : "Maximum size of the PDP cache, in megabytes (Property name:
 org.forgerock.agents.pdp.cache.total.size.mb).",
          "propertyOrder" : 13600,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "integer",
              "required" : false
            }
          }
        },
        "policyCacheSize" : {
          "title" : "Policy Cache Size",
          "description" : "The maximum number of sessions, i.e. distinct users, stored in the
 policy evaluation cache at any one time. (property: org.forgerock.agents.policy.cache.session.size)
 <br>Required Agent Restart",
          "propertyOrder" : 14000,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "integer",
              "required" : false
            }
          }
        },
        "fragmentRelayUri" : {
          "title" : "Fragment Relay URI",
          "description" : "To enable unauthenticated fragment retention within incoming requests, set
 this property to a valid dummy URI within the Agent application.<br>Example: /agentapp/pre-authn-
fragment-capture <br>(property: org.forgerock.agents.authn.fragment.relay.uri) (Agent 5.7+ only)",
          "propertyOrder" : 13090,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
```

```
        }
      },
      "alternativeAgentProtocol" : {
        "title" : "Alternative Agent Protocol",
        "description" : "Protocol being used (http/https) by the client browsers to communicate with
the Agent protected server if different from the actual protocol used by the server. (property name:
org.forgerock.agents.agent.protocol) ",
        "propertyOrder" : 4300,
        "type" : "object",
        "exampleValue" : "",
        "properties" : {
          "inherited" : {
            "type" : "boolean",
            "required" : true
          },
          "value" : {
            "type" : "string",
            "required" : false
          }
        }
      },
      "postDataStickySessionKeyValue" : {
        "title" : "PDP Stickysession key-value",
        "description" : "The provided key-value pair will be used for adding to the URL or creating
the cookie. <br>Example: <br>Set 'lb=server1' to append to the querystring or to have 'lb' cookie
with 'server1' value. (property name: org.forgerock.agents.pdp.sticky.session.value)",
        "propertyOrder" : 13500,
        "type" : "object",
        "exampleValue" : "",
        "properties" : {
          "inherited" : {
            "type" : "boolean",
            "required" : true
          },
          "value" : {
            "type" : "string",
            "required" : false
          }
        }
      },
      "missingPostDataPreservationEntryUri" : {
        "title" : "Missing PDP entry URI",
        "description" : "An application-specific URI Map that is used in case the referenced
PDP entry cannot be found in the local cache (due to ttl). In such cases it will redirect
to the specified URI, otherwise it will show a HTTP 403 Forbidden error. (property name:
org.forgerock.agents.pdp.noentry.url.map)<br>Examples: <br>To set a redirect target for application
BankApp: enter Bankapp in Map Key field and enter a redirect URI in corresponding Map Value field.",
        "propertyOrder" : 13200,
        "items" : {
          "type" : "string"
        },
        "type" : "object",
        "exampleValue" : "",
        "properties" : {
          "inherited" : {
            "type" : "boolean",
            "required" : true
          },
          "value" : {
```

```
              "type" : "array",
              "required" : false
            }
          }
        },
        "sessionCacheTTL" : {
          "title" : "Session Cache TTL",
          "description" : "This sets the time in minutes after which entries in the session cache
 will timeout and be purged.  If an entry is not cached, the Agent will need to retrieve session
 information from AM, hence by default the timeout is much longer than for the policy cache.
 (property: org.forgerock.agents.session.cache.ttl.minutes) <br>Required Agent Restart",
          "propertyOrder" : 13700,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "integer",
              "required" : false
            }
          }
        },
        "postDataCacheTtl" : {
          "title" : "PDP Cache TTL in Milliseconds",
          "description" : "This value tells how long a given POST entry should be stored in the
 local cache (in milliseconds), default value is 300000. DEPRECATED: use \"PDP Cache TTL in Minutes
\" instead (property name: com.sun.identity.agents.config.postdata.preserve.cache.entry.ttl)
 <br>Required Agent Restart",
          "propertyOrder" : 13310,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "integer",
              "required" : false
            }
          }
        },
        "policyClientPollingInterval" : {
          "title" : "Policy Cache TTL",
          "description" : "This sets the time in minutes after which entries in the policy cache will
 timeout and be purged. (property name: org.forgerock.agents.policy.cache.ttl.minutes) <br>Required
 Agent Restart",
          "propertyOrder" : 13950,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
```

```
              "type" : "integer",
              "required" : false
            }
          }
        },
        "jwtCacheTTL" : {
          "title" : "JWT Cache TTL",
          "description" : "This sets the time in minutes after which entries in the JWT cache will
timeout and be purged.  Since all JWTs in the cache have been parsed, and parsing is a CPU intensive
process, having a large timeout on this cache is advantageous and will save CPU cycles reparsing
already seen JWTs (property: org.forgerock.agents.jwt.cache.ttl.minutes) <br>Required Agent Restart",
          "propertyOrder" : 13800,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "integer",
              "required" : false
            }
          }
        },
        "possibleXssCodeElements" : {
          "title" : "Possible XSS code elements",
          "description" : "If one of these strings occurs in the request, the client is redirected to
an error page. (property name: org.forgerock.agents.xss.code.element.list) ",
          "propertyOrder" : 12800,
          "items" : {
            "type" : "string"
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "array",
              "required" : false
            }
          }
        },
        "jwtCacheSize" : {
          "title" : "JWT Cache Size",
          "description" : "The maximum number of entries in the JWT cache. (property:
org.forgerock.agents.jwt.cache.size) <br>Required Agent Restart",
          "propertyOrder" : 13810,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
```

```
              "type" : "integer",
              "required" : false
            }
          }
        }
      }
    },
    "miscJ2EEAgentConfig" : {
      "type" : "object",
      "title" : "Miscellaneous",
      "propertyOrder" : 4,
      "properties" : {
        "gotoUrl" : {
          "title" : "Goto Url",
          "description" : "This is a URL used in rare circumstances where the Agent has nowhere
else to go.  For instance if the user requests a resource, authenticates for the first time,
then presses the back button and the administrator hasn't set up the authn fail URL. (property:
org.forgerock.agents.default.goto.url)",
          "propertyOrder" : 19200,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "unwantedHttpUrlParams" : {
          "title" : "Remove Query Parameters",
          "description" : "Specifies a list of query parameters to be removed from a URL for policy
decision and caching purposes. The property has the format [Domain/path] | parameter[,parameter...]
with no spaces between values (property: org.forgerock.agents.unwanted.http.url.param.list)
<br>Example: myapp.example.com/customers|location,lang",
          "propertyOrder" : 19500,
          "items" : {
            "type" : "string"
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "array",
              "required" : false
            }
          }
        },
        "loginReasonParameterName" : {
          "title" : "Login Reason Parameter Name",
          "description" : "Property to say why the user is being asked to login, the agent will (in
custom login mode ONLY) pass the named parameter to the custom login endpoint, with an appropriate
```

```
value.  Note that this property is not enabled by default as this additional information represents
an information leak. Default reasons: NO_TOKEN, JWT_INVALID, TOKEN_EXPIRED, EXCEPTION. (property:
org.forgerock.agents.login.reason.parameter.name)",
         "propertyOrder" : 18700,
         "type" : "object",
         "exampleValue" : "",
         "properties" : {
           "inherited" : {
             "type" : "boolean",
             "required" : true
           },
           "value" : {
             "type" : "string",
             "required" : false
           }
         }
       },
       "authFailReasonParameterRemapper" : {
         "title" : "Authentication Fail Reason Parameter Value Map",
         "description" : "This map allows some of the possible reasons to be
mapped to arbitrary values. When empty, will use default values. (property:
org.forgerock.agents.authn.fail.reason.remapper)",
         "propertyOrder" : 19100,
         "patternProperties" : {
           ".*" : {
             "type" : "string"
           }
         },
         "type" : "object",
         "exampleValue" : "",
         "properties" : {
           "inherited" : {
             "type" : "boolean",
             "required" : true
           },
           "value" : {
             "type" : "object",
             "required" : false
           }
         }
       },
       "gotoParameterName" : {
         "title" : "Goto Parameter Name",
         "description" : "This is the name of the HTTP query \"goto\" parameter. It is not
recommended to change it. (property name: com.sun.identity.agents.config.redirect.param) ",
         "propertyOrder" : 3600,
         "type" : "object",
         "exampleValue" : "",
         "properties" : {
           "inherited" : {
             "type" : "boolean",
             "required" : true
           },
           "value" : {
             "type" : "string",
             "required" : false
           }
         }
       },
```

```
        "localeCountry" : {
          "title" : "Locale Country",
          "description" : "(property name: org.forgerock.agents.locale.country) <br>Required Agent
 Restart",
          "propertyOrder" : 1400,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "authFailReasonParameterName" : {
          "title" : "Authentication Fail Reason Parameter Name",
          "description" : "If this property is defined, the agent will pass the named parameter
 to a custom page (defined by \"Authentication Fail Reason Url\") saying why authentication
 failed.  The reason can be very detailed and users may want to use the \"Authentication
 Fail Reason Parameter Value Map\" to give custom detail, otherwise these default values
 will be used: AUTHN_BOOKKEEPING_COOKIE_MISSING, NONCE_MISSING, EXCEPTION (property:
 org.forgerock.agents.authn.fail.reason.parameter.name)",
          "propertyOrder" : 19000,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "wantedHttpUrlParams" : {
          "title" : "Retain Query Parameters",
          "description" : "Specifies a list of query parameters to be retained (other parameters
 will be removed) from a URL for policy decision and caching purposes. The property has the
 format [Domain/path] | parameter[,parameter...] with no spaces between values. (property:
 org.forgerock.agents.wanted.http.url.param.list) <br>Example: myapp.example.com/customers|
location,lang",
          "propertyOrder" : 19300,
          "items" : {
            "type" : "string"
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
```

```
              "type" : "array",
              "required" : false
            }
          }
        },
        "loginReasonMap" : {
          "title" : "Login Reason Value Map",
          "description" : "This map allows some of the possible reasons to be mapped to
 arbitrary values, when empty will be used default values(see: \"Login Reason Parameter Name
\" description). LOGIN REASON=CUSTOM VALUE e.g. [JWT_INVALID]=corrupted_token. (property:
 org.forgerock.agents.login.reason.remapper)",
          "propertyOrder" : 18800,
          "patternProperties" : {
            ".*" : {
              "type" : "string"
            }
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "object",
              "required" : false
            }
          }
        },
        "legacyUserAgentSupport" : {
          "title" : "Legacy User Agent Support Enable",
          "description" : "Enables support for legacy user agents (browser). (property name:
 org.forgerock.agents.legacy.support.enabled) ",
          "propertyOrder" : 6700,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : false
            }
          }
        },
        "serviceResolverClass" : {
          "title" : "Service Resolver Class Name",
          "description" : "Name of the service resolver class to change in order
 to instantiate own service resolver and overriding default ones <br>(property:
 org.forgerock.agents.service.resolver.class.name) (Agent 5.6.2+ only) <br> Agent restart is
 required",
          "propertyOrder" : 19700,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
```

```
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "wantedHttpUrlRegexParams" : {
          "title" : "Regular Expression Retain Query Parameters",
          "description" : "Specifies a list of regular expressions the agent uses to match query
parameters to be retained for policy decision and caching purposes. The property has the format
[Domain/path] | regular_expression[,regular_expression...] with no spaces between values. (property:
org.forgerock.agents.wanted.http.url.params.regex.list)",
          "propertyOrder" : 19400,
          "items" : {
            "type" : "string"
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "array",
              "required" : false
            }
          }
        },
        "authFailReasonUrl" : {
          "title" : "Authentication Fail Reason Url",
          "description" : "This property allows administrators to set the URL/URI of a web page that
says that authentication failed and which may, using the login fail reason parameter, explain why.
(property: org.forgerock.agents.authn.fail.url)",
          "propertyOrder" : 18900,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "portCheckEnabled" : {
          "title" : "Port Check Enable",
          "description" : "Indicates if port check functionality is enabled or disabled. (property
name: org.forgerock.agents.port.check.enabled) ",
          "propertyOrder" : 7200,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
```

```
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : false
            }
          }
        },
        "legacyRedirectUri" : {
          "title" : "Legacy User Agent Redirect URI",
          "description" : "An intermediate URI used by the Agent to redirect legacy user agent
requests. (property name: org.forgerock.agents.legacy.redirect.uri) ",
          "propertyOrder" : 6900,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "portCheckSetting" : {
          "title" : "Port Check Setting",
          "description" : "Map of port versus protocol entries with the key being the listening port
number and value being the listening protocol to be used by the Agent to identify requests with
invalid port numbers. (property name: org.forgerock.agents.port.check.map)  <br> Example: <br> To
map port 80 to protocol http: enter 80 in Map Key field, and enter http in Corresponding Map Value
field.",
          "propertyOrder" : 7400,
          "patternProperties" : {
            ".*" : {
              "type" : "string"
            }
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "object",
              "required" : false
            }
          }
        },
        "unwantedHttpUrlRegexParams" : {
          "title" : "Regular Expression Remove Query Parameters",
          "description" : "Specifies a list of regular expressions the agent uses to match query
parameters to be removed from a URL for policy decision and caching purposes. The property has the
```

```
format [Domain/path] | regular_expression[,regular_expression...] with no spaces between values.
(property: org.forgerock.agents.unwanted.http.url.params.regex.list)",
         "propertyOrder" : 19600,
         "items" : {
           "type" : "string"
         },
         "type" : "object",
         "exampleValue" : "",
         "properties" : {
           "inherited" : {
             "type" : "boolean",
             "required" : true
           },
           "value" : {
             "type" : "array",
             "required" : false
           }
         }
       },
       "legacyUserAgentList" : {
         "title" : "Legacy User Agent List",
         "description" : "List of user agent header values that identify legacy
browsers. Entries in this list can have wild card character '*'. (property name:
org.forgerock.agents.legacy.user.agent.list) ",
         "propertyOrder" : 6800,
         "items" : {
           "type" : "string"
         },
         "type" : "object",
         "exampleValue" : "",
         "properties" : {
           "inherited" : {
             "type" : "boolean",
             "required" : true
           },
           "value" : {
             "type" : "array",
             "required" : false
           }
         }
       },
       "portCheckFile" : {
         "title" : "Port Check File",
         "description" : "Name or complete path of a file that has the necessary content needed to
handle requests that need port correction. (property name: org.forgerock.agents.port.check.file) ",
         "propertyOrder" : 7300,
         "type" : "object",
         "exampleValue" : "",
         "properties" : {
           "inherited" : {
             "type" : "boolean",
             "required" : true
           },
           "value" : {
             "type" : "string",
             "required" : false
           }
         }
       },
```

```
       "ignorePathInfo" : {
         "title" : "Ignore Path Info in Request URL",
         "description" : "The path info will be stripped from the request URL while doing Not
Enforced List check and url policy evaluation if the value is set to true. (property name:
com.sun.identity.agents.config.ignore.path.info)",
         "propertyOrder" : 18600,
         "type" : "object",
         "exampleValue" : "",
         "properties" : {
           "inherited" : {
             "type" : "boolean",
             "required" : true
           },
           "value" : {
             "type" : "boolean",
             "required" : false
           }
         }
       },
       "localeLanguage" : {
         "title" : "Locale Language",
         "description" : "(property name: org.forgerock.agents.locale.language) <br>Required Agent
Restart",
         "propertyOrder" : 1300,
         "type" : "object",
         "exampleValue" : "",
         "properties" : {
           "inherited" : {
             "type" : "boolean",
             "required" : true
           },
           "value" : {
             "type" : "string",
             "required" : false
           }
         }
       }
     }
   },
   "applicationJ2EEAgentConfig" : {
     "type" : "object",
     "title" : "Application",
     "propertyOrder" : 1,
     "properties" : {
       "profileAttributeFetchMode" : {
         "title" : "Profile Attribute Fetch Mode",
         "description" : "The mode of fetching profile attributes. (property name:
com.sun.identity.agents.config.profile.attribute.fetch.mode) ",
         "propertyOrder" : 8700,
         "type" : "object",
         "exampleValue" : "",
         "properties" : {
           "inherited" : {
             "type" : "boolean",
             "required" : true
           },
           "value" : {
             "type" : "string",
             "required" : false
```

```
            }
          }
        },
        "logoutRequestParameters" : {
          "title" : "Logout Request Parameter",
          "description" : "An application-specific Map that identifies a parameter
which when present in the HTTP request indicates a logout event. (property name:
org.forgerock.agents.logout.request.param.map)  <br>Valid key: the web application name. <br>Valid
value: the logout request parameter. <br>For this property, a global value can be set to apply to
all the applications that don't have their own specific logout request parameter.   <br> Examples:
<br>To set a global application logout request parameter: leave Map Key field empty, and enter the
global application logout request parameter logoutparam in Corresponding Map Value field. <br> To set
the logout request parameter for application BankApp: enter BankApp in Map Key field, and enter the
logout request parameter logoutparam in Corresponding Map Value field.",
          "propertyOrder" : 6100,
          "patternProperties" : {
            ".*" : {
              "type" : "string"
            }
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "object",
              "required" : false
            }
          }
        },
        "invertNotEnforcedIps" : {
          "title" : "Invert Not Enforced IPs",
          "description" : "Client IP Addresses to invert protection of IP
addresses listed in the related Not Enforced Client IP List. (property name:
org.forgerock.agents.notenforced.ip.invert.enabled) ",
          "propertyOrder" : 8000,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : false
            }
          }
        },
        "notEnforcedIps" : {
          "title" : "Not Enforced Client IP List",
          "description" : "No authentication and authorization protection from agent
are required for the requests coming from these client IP addresses. (property name:
org.forgerock.agents.notenforced.ip.list)  <br> Examples: <br> 192.18.145.* <br> 192.18.146.123",
          "propertyOrder" : 7900,
          "items" : {
```

```
            "type" : "string"
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "array",
              "required" : false
            }
          }
        },
        "continuousSecurityCookies" : {
          "title" : "Continuous Security Cookies",
          "description" : "The name of the cookies to be sent as part of the payload during policy
 evaluation, which can be accessed via the 'environment' variable in a policy script. The 'key' is
 the name of the cookie to be sent, and the 'value' is the name which it will appear as in the policy
 evaluation script. It is possible to map multiple cookies to the same name (they will simply appear
 as an array in the evaluation script). If the cookie doesn't exist, then the empty string will be
 sent.",
          "propertyOrder" : 3210,
          "patternProperties" : {
            ".*" : {
              "type" : "string"
            }
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "object",
              "required" : false
            }
          }
        },
        "applicationLogoutUris" : {
          "title" : "Application Logout URI",
          "description" : "An application-specific Map that identifies a request URI which indicates
 a logout event. (property name: org.forgerock.agents.logout.endpoint.map) <br>Valid key: the web
 application name. <br>Valid value: the application logout URI. <br>For this property, a global value
 can be set to apply to all the applications that don't have their own specific logout URI.  <br>
 Examples: <br>To set a global application logout URI: leave Map Key field empty, and enter the global
 application logout URI /logout.jsp in Corresponding Map Value field. <br> To set the logout URI for
 application BankApp: enter BankApp in Map Key field, and enter the application logout URI /BankApp/
logout.jsp in Corresponding Map Value field.",
          "propertyOrder" : 6000,
          "patternProperties" : {
            ".*" : {
              "type" : "string"
            }
          },
          "type" : "object",
```

```
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "object",
              "required" : false
            }
          }
        },
        "sessionAttributeFetchMode" : {
          "title" : "Session Attribute Fetch Mode",
          "description" : "The mode of fetching session attributes. (property name:
com.sun.identity.agents.config.session.attribute.fetch.mode) ",
          "propertyOrder" : 8900,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "notEnforcedIpsCacheEnabled" : {
          "title" : "Not Enforced IP Cache Flag",
          "description" : "Enable caching of not-enforced IP list evaluation results. (property name:
org.forgerock.agents.notenforced.ip.cache.enabled) ",
          "propertyOrder" : 8100,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : false
            }
          }
        },
        "cookieAttributeUrlEncoded" : {
          "title" : "Attribute Cookie Encode",
          "description" : "Indicates if the value of the attribute should be URL encoded before being
set as a cookie. (property name: org.forgerock.agents.attribute.cookie.encode.enabled) ",
          "propertyOrder" : 8500,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
```

```
            },
            "value" : {
              "type" : "boolean",
              "required" : false
            }
          }
        },
        "logoutEntryUri" : {
          "title" : "Logout Entry URI",
          "description" : "An application-specific Map that identifies a URI to be used as an entry
 point after successful logout and subsequent successful authentication if applicable. (property name:
 org.forgerock.agents.logout.goto.map) <br>Valid key: the web application name. <br>Valid value: the
 logout entry URI. <br>For this property, a global value can be set to apply to all the applications
 that don't have their own specific logout entry URI.   <br> Examples: <br>To set a global application
 logout entry URI: leave Map Key field empty, and enter the global application logout entry URI /
welcome.html in Corresponding Map Value field. <br> To set the logout entry URI for application
 BankApp: enter BankApp in Map Key field, and enter the logout entry URI /BankApp/welcome.html in
 Corresponding Map Value field.",
          "propertyOrder" : 6300,
          "patternProperties" : {
            ".*" : {
              "type" : "string"
            }
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "object",
              "required" : false
            }
          }
        },
        "cookieAttributeMultiValueSeparator" : {
          "title" : "Cookie Separator Character",
          "description" : "Character that will be used to separate multiple
 values of the same attribute when it is being set as a cookie. (property name:
 org.forgerock.agents.attribute.cookie.separator) ",
          "propertyOrder" : 8300,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "responseAttributeFetchMode" : {
          "title" : "Response Attribute Fetch Mode",
```

```
          "description" : "The mode of fetching policy response attributes. (property name:
com.sun.identity.agents.config.response.attribute.fetch.mode) ",
          "propertyOrder" : 9100,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "notEnforcedIpsCacheSize" : {
          "title" : "Not Enforced IP Cache Size",
          "description" : "Size of the cache to be used if Not Enforced IP Cache Flag is enabled.
(property name: org.forgerock.agents.notenforced.ip.cache.size) ",
          "propertyOrder" : 8200,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "integer",
              "required" : false
            }
          }
        },
        "notEnforcedFavicon" : {
          "title" : "Not Enforced Favicon",
          "description" : "This flag, if enabled, automatically adds \"*/favicon.ico\" to
the not enforced list.  This can help to avoid odd situations in which a user is required to
log in after logging out, just because favicon.ico has been requested by browser. (property:
org.forgerock.agents.auto.not.enforce.favicon.enabled) <br>Required Agent Restart",
          "propertyOrder" : 7650,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : false
            }
          }
        },
        "notEnforcedRuleCompoundSeparator" : {
          "title" : "Not Enforced Compound Rule Separator",
          "description" : "Specifies a separator for not enforced compound rules. The format for
compound rules requires a list of IP rules, a separator (by default the | character), and a list of
```

```
URI rules. <br>Example, GET 192.168.1.1-192.168.4.3 | /images/* <br>Configure a different separator
(for example, &&) when working with the REGEX keyword to avoid invalid regular expressions.",
         "propertyOrder" : 7450,
         "type" : "object",
         "exampleValue" : "",
         "properties" : {
           "inherited" : {
             "type" : "boolean",
             "required" : true
           },
           "value" : {
             "type" : "string",
             "required" : false
           }
         }
       },
       "resourceAccessDeniedUri" : {
         "title" : "Resource Access Denied URI",
         "description" : "An application-specific Map that identifies a URI of the customized access
denied page. (property name: org.forgerock.agents.access.denied.uri.map) <br>Valid key: the web
application name. <br>Valid value: the customized application access denied page URI. <br>For this
property, a global value can be set to apply to all the applications that don't have their own
specific access denied page.  <br> Examples: <br>To set a global access denied page: leave Map Key
field empty, and enter the global access denied page URI /sample/accessdenied.html in Corresponding
Map Value field. <br> To set the access denied page URI for application BankApp: enter BankApp
in Map Key field, and enter the application access denied page URI /BankApp/accessdenied.html in
Corresponding Map Value field.",
         "propertyOrder" : 2700,
         "patternProperties" : {
           ".*" : {
             "type" : "string"
           }
         },
         "type" : "object",
         "exampleValue" : "",
         "properties" : {
           "inherited" : {
             "type" : "boolean",
             "required" : true
           },
           "value" : {
             "type" : "object",
             "required" : false
           }
         }
       },
       "profileAttributeMap" : {
         "title" : "Profile Attribute Mapping",
         "description" : "Maps the profile attributes to be populated under specific names for the
currently authenticated user. (property name: org.forgerock.agents.profile.attribute.map)  <br>
Example: <br> To populate the value of profile attribute cn under name CUSTOM-Common-Name: enter cn
in Map Key field, and enter CUSTOM-Common-Name in Corresponding Map Value field. <br> To populate
the value of profile attribute mail under name CUSTOM-Email: enter mail in Map Key field, and enter
CUSTOM-Email in Corresponding Map Value field.",
         "propertyOrder" : 8800,
         "patternProperties" : {
           ".*" : {
             "type" : "string"
           }
```

```
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "object",
              "required" : false
            }
          }
        },
        "headerAttributeDateFormat" : {
          "title" : "Fetch Attribute Date Format",
          "description" : "Format of date attribute values to be used when the attribute is
 being set as HTTP header. Format is based on java.text.SimpleDateFormat. (property name:
 org.forgerock.agents.attribute.date.format) ",
          "propertyOrder" : 8400,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "notEnforcedUris" : {
          "title" : "Not Enforced URIs",
          "description" : "List of URIs for which protection is not enforced by the Agent. (property
 name: org.forgerock.agents.notenforced.uri.list)  <br> Examples: <br> /BankApp/public/* <br> /
BankApp/images/*",
          "propertyOrder" : 7500,
          "items" : {
            "type" : "string"
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "array",
              "required" : false
            }
          }
        },
        "responseAttributeMap" : {
          "title" : "Response Attribute Mapping",
          "description" : "Maps the policy response attributes to be populated under specific names
 for the currently authenticated user. (property name: org.forgerock.agents.response.attribute.map)
```

```
 <br> Example: <br> To populate the value of response attribute uid under name CUSTOM-USER-NAME: enter
 uid in Map Key field, and enter CUSTOM-USER-NAME in Corresponding Map Value field.",
          "propertyOrder" : 9200,
          "patternProperties" : {
            ".*" : {
              "type" : "string"
            }
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "object",
              "required" : false
            }
          }
        },
        "continuousSecurityHeaders" : {
          "title" : "Continuous Security Headers",
          "description" : "The name of the headers in the user's original request, that will be sent
 as part of the payload during policy evaluation, which can then be accessed via the 'environment'
 variable in a policy script. The 'key' is the name of the header to be sent, and the 'value' is the
 name which it will appear as in the policy evaluation script.It is possible to map multiple headers
 to the same name (they will simply appear as an array in the evaluation script). If the header
 doesn't exist, then the empty string will be sent.",
          "propertyOrder" : 3211,
          "patternProperties" : {
            ".*" : {
              "type" : "string"
            }
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "object",
              "required" : false
            }
          }
        },
        "loginFormUri" : {
          "title" : "Login Form URI",
          "description" : "List of absolute URIs corresponding to an application's web.xml form-login-
page element. (property name: com.sun.identity.agents.config.login.form)  <br> Example: <br> /BankApp/
jsp/login.jsp",
          "propertyOrder" : 2800,
          "items" : {
            "type" : "string"
          },
          "type" : "object",
          "exampleValue" : "",
```

```
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "array",
              "required" : false
            }
          }
        },
        "notEnforcedUrisCacheSize" : {
          "title" : "Not Enforced URIs Cache Size",
          "description" : "Size of the cache to be used if caching of not enforced URI list evaluation
results is enabled. (property name: org.forgerock.agents.notenforced.uri.cache.size) ",
          "propertyOrder" : 7800,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "integer",
              "required" : false
            }
          }
        },
        "notEnforcedUrisCacheEnabled" : {
          "title" : "Not Enforced URIs Cache Enabled",
          "description" : "Enables the caching of the Not Enforced URIs list evaluation results.
(property name: org.forgerock.agents.notenforced.uri.cache.enabled) ",
          "propertyOrder" : 7700,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : false
            }
          }
        },
        "sessionAttributeMap" : {
          "title" : "Session Attribute Mapping",
          "description" : "Maps the session attributes to be populated under specific names for the
currently authenticated user. (property name: org.forgerock.agents.session.attribute.map)   <br>
Example: <br>  To populate the value of session attribute UserToken under name CUSTOM-userid: enter
UserToken in Map Key field, and enter CUSTOM-userid in Corresponding Map Value field.",
          "propertyOrder" : 9000,
          "patternProperties" : {
            ".*" : {
              "type" : "string"
            }
          },
```

```
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "object",
              "required" : false
            }
          }
        },
        "invertNotEnforcedUris" : {
          "title" : "Invert Not Enforced URIs",
          "description" : "Inverts protection of  URIs specified in Not Enforced URIs list. When set
to true, it indicates that the URIs specified should be enforced and all other URIs should be not
enforced by the Agent. (property name: org.forgerock.agents.notenforced.uri.invert.enabled) ",
          "propertyOrder" : 7600,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : false
            }
          }
        },
        "logoutIntrospection" : {
          "title" : "Logout Introspect Enabled",
          "description" : "Allows the Agent to search HTTP request body to locate logout parameter.
(property name: org.forgerock.agents.logout.introspection.enabled) ",
          "propertyOrder" : 6200,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : false
            }
          }
        }
      }
    },
    "globalJ2EEAgentConfig" : {
      "type" : "object",
      "title" : "Global",
      "propertyOrder" : 0,
      "properties" : {
        "fqdnMapping" : {
          "title" : "FQDN Virtual Host Map",
```

```
          "description" : "Maps virtual, invalid, or partial hostnames, and IP addresses to the
FQDN to access protected resources. (property name: org.forgerock.agents.fqdn.map)  <br> Examples:
<br>  To map the partial hostname myserver to myserver.mydomain.com: enter myserver in the Map
Key field and myserver.mydomain.com in the Corresponding Map Value field. To map a virtual server
rst.hostname.com that points to the actual server abc.hostname.com: enter valid1 in the Map Key field
and rst.hostname.com in the Corresponding Map Value field.",
          "propertyOrder" : 6600,
          "patternProperties" : {
            ".*" : {
              "type" : "string"
            }
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "object",
              "required" : false
            }
          }
        },
        "localAuditRotationSize" : {
          "title" : "Local Audit Log Rotation Size",
          "description" : "Size limit when a local audit log file is rotated to a new file. (property
name: com.sun.identity.agents.config.local.log.size) ",
          "propertyOrder" : 1900,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "integer",
              "required" : false
            }
          }
        },
        "agentSessionChangeNotificationsEnabled" : {
          "title" : "Session Logout Notification ",
          "description" : "Flag to indicate whether the Agent will subscribe
to session logout notifications (via websockets) from AM. (property:
org.forgerock.agents.session.change.notifications.enabled)",
          "propertyOrder" : 12110,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : false
```

```
            }
          }
        },
        "localAuditLogRotation" : {
          "title" : "Rotate Local Audit Log",
          "description" : "Flag to indicate that audit log files should be rotated when reaching a
certain size. (property name: org.forgerock.agents.local.audit.log.rotation.enabled) ",
          "propertyOrder" : 1800,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : false
            }
          }
        },
        "redirectAttemptLimitCookieName" : {
          "title" : "Redirect Attempt Cookie Name",
          "description" : "Agent tries to detect redirect loops while authenticating, which would
normally indicate a cookie domain problem.  The Agent does this by using a cookie to holds the
current redirection count. (property: org.forgerock.agents.redirect.cookie.name)",
          "propertyOrder" : 7150,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "configurationReloadInterval" : {
          "title" : "Configuration Reload Interval",
          "description" : "Only used when websocket notifications are disabled, specifies
interval in seconds after which config is reloaded automatically by the Agent. (property name:
org.forgerock.agents.config.reload.seconds) ",
          "propertyOrder" : 1200,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "integer",
              "required" : false
            }
          }
        },
```

```
       "debugLogfileRotationMinutes" : {
         "title" : "Debug File Rotation Time",
         "description" : "This is the time in minutes after which log file rotation will occur.
(property: org.forgerock.agents.debug.rotation.time.minutes)",
         "propertyOrder" : 10040,
         "type" : "object",
         "exampleValue" : "",
         "properties" : {
           "inherited" : {
             "type" : "boolean",
             "required" : true
           },
           "value" : {
             "type" : "integer",
             "required" : false
           }
         }
       },
       "agentConfigChangeNotificationsEnabled" : {
         "title" : "Agent Configuration Change Notification",
         "description" : "Enable agent to receive notification messages
(via websockets) from AM server for configuration changes. (property name:
org.forgerock.agents.config.change.notifications.enabled) ",
         "propertyOrder" : 12100,
         "type" : "object",
         "exampleValue" : "",
         "properties" : {
           "inherited" : {
             "type" : "boolean",
             "required" : true
           },
           "value" : {
             "type" : "boolean",
             "required" : false
           }
         }
       },
       "customResponseHeader" : {
         "title" : "Custom Response Header",
         "description" : "Map specifies the custom headers that are set by the Agent on the client
browser. The key is the header name and the value represents the header value. (property name:
org.forgerock.agents.response.header.map)  <br> Example: <br>  To set the custom header Cache-Control
to value no-cache: enter Cache-Control in Map Key field, and enter no-cache in Corresponding Map
Value field.",
         "propertyOrder" : 7000,
         "patternProperties" : {
           ".*" : {
             "type" : "string"
           }
         },
         "type" : "object",
         "exampleValue" : "",
         "properties" : {
           "inherited" : {
             "type" : "boolean",
             "required" : true
           },
           "value" : {
             "type" : "object",
```

```
              "required" : false
            }
          }
        },
        "debugLevel" : {
          "title" : "Agent Debug Level",
          "description" : "Specifies type of agent debug messages to log. (property name:
com.iplanet.services.debug.level) ",
          "propertyOrder" : 10000,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "preAuthCookieMaxAge" : {
          "title" : "Pre-Authenticated Cookie Max Age",
          "description" : "This is the amount of time in seconds before the pre-authn cookie will
timeout. (property: org.forgerock.agents.authn.cookie.max.age.seconds)",
          "propertyOrder" : 11220,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "integer",
              "required" : false
            }
          }
        },
        "debugLogfileRetentionCount" : {
          "title" : "Debug File Rotation Retention Count",
          "description" : "This is the number of log files to retain after rotation, so for example,
setting it to 10 would give you one current debug file and nine older (rotated) files. (property:
org.forgerock.agents.debug.retention.count)",
          "propertyOrder" : 10050,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "integer",
              "required" : false
            }
          }
        },
```

```
       "fqdnCheck" : {
         "title" : "FQDN Check",
         "description" : "Enables checking of fqdn default value and fqdn map values. (property name:
org.forgerock.agents.fqdn.check.enabled) ",
         "propertyOrder" : 6400,
         "type" : "object",
         "exampleValue" : "",
         "properties" : {
           "inherited" : {
             "type" : "boolean",
             "required" : true
           },
           "value" : {
             "type" : "boolean",
             "required" : false
           }
         }
       },
       "webSocketConnectionIntervalInMinutes" : {
         "title" : "Web Socket Connection Interval",
         "description" : "Interval in minutes by which agents reopen their web socket
connection to ensure a fair distribution of connections across AM servers. (property:
org.forgerock.agents.balance.websocket.interval.minutes).",
         "propertyOrder" : 12120,
         "type" : "object",
         "exampleValue" : "",
         "properties" : {
           "inherited" : {
             "type" : "boolean",
             "required" : true
           },
           "value" : {
             "type" : "integer",
             "required" : false
           }
         }
       },
       "preAuthCookieName" : {
         "title" : "Pre-Authenticated Cookie Name",
         "description" : "Specifies the name of the cookie the agent uses to track the progress of
authentication with AM. (property: org.forgerock.agents.authn.cookie.name)",
         "propertyOrder" : 11210,
         "type" : "object",
         "exampleValue" : "",
         "properties" : {
           "inherited" : {
             "type" : "boolean",
             "required" : true
           },
           "value" : {
             "type" : "string",
             "required" : false
           }
         }
       },
       "httpSessionBinding" : {
         "title" : "HTTP Session Binding",
```

```
          "description" : "If true will invalidate the http session when login has failed,
user has no SSO session, or principal user name does not match SSO user name. (property name:
org.forgerock.agents.http.session.binding.enabled) ",
          "propertyOrder" : 3500,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : false
            }
          }
        },
        "userTokenName" : {
          "title" : "User Token Name",
          "description" : "Session property name for user-ID of the authenticated user in session.
(property name: org.forgerock.agents.userid.mapping.mode.use.session.property.name) ",
          "propertyOrder" : 900,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "userpassword" : {
          "title" : "Password",
          "description" : "",
          "propertyOrder" : 100,
          "required" : true,
          "type" : "string",
          "format" : "password",
          "exampleValue" : ""
        },
        "auditAccessType" : {
          "title" : "Audit Access Types",
          "description" : "Types of messages to log based on user URL access attempts. (property name:
org.forgerock.agents.audit.what) ",
          "propertyOrder" : 1500,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
```

```
            }
          }
        },
        "userMappingMode" : {
          "title" : "User Mapping Mode",
          "description" : "Specifies mechanism agent uses to determine user-ID. (property name:
org.forgerock.agents.user.mapping.mode) ",
          "propertyOrder" : 600,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "repositoryLocation" : {
          "title" : "Location of Agent Configuration Repository",
          "description" : "Indicates agent's configuration located either on agent's host or centrally
on AM server (property: org.forgerock.agents.config.location).",
          "propertyOrder" : 400,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "status" : {
          "title" : "Status",
          "description" : "Status of the agent configuration.",
          "propertyOrder" : 200,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : true
            }
          }
        },
        "localAuditLogfileRetentionCount" : {
          "title" : "Audit Logfile Retention Count",
          "description" : "The number of audit log files to retain after rotation has occurred.
(property: org.forgerock.agents.local.audit.log.retention.count)",
          "propertyOrder" : 2100,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
```

```
            "value" : {
              "type" : "integer",
              "required" : false
            }
          }
        },
        "fqdnDefault" : {
          "title" : "FQDN Default",
          "description" : "Fully qualified hostname that the users should use in order to access
resources. (property name: org.forgerock.agents.fqdn.default) ",
          "propertyOrder" : 6500,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "loginAttemptLimitCookieName" : {
          "title" : "Login Attempt Limit Cookie Name",
          "description" : "The name of the cookie used to record the number of login attempts.
(property: org.forgerock.agents.login.counter.cookie.name)",
          "propertyOrder" : 4500,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "jwtName" : {
          "title" : "JWT Cookie Name",
          "description" : "The name used by the agent to set the OIDC JWT on the user's browser.
(property: org.forgerock.agents.jwt.cookie.name)",
          "propertyOrder" : 11201,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
```

```
      },
      "redirectAttemptLimit" : {
        "title" : "Redirect Attempt Limit",
        "description" : "Number of successive single point redirects that a user can make using a
single browser session which will trigger the blocking of the user request. Set to 0 to disable this
feature. (property name: org.forgerock.agents.redirect.attempt.limit) ",
        "propertyOrder" : 7100,
        "type" : "object",
        "exampleValue" : "",
        "properties" : {
          "inherited" : {
            "type" : "boolean",
            "required" : true
          },
          "value" : {
            "type" : "integer",
            "required" : false
          }
        }
      },
      "agentgroup" : {
        "title" : "Group",
        "description" : "Add the agent to a group to allow inheritance of property values from the
group. <br>Changing the group will update inherited property values. <br>Inherited property values
are copied to the agent.",
        "propertyOrder" : 50,
        "required" : false,
        "type" : "string",
        "exampleValue" : ""
      },
      "userAttributeName" : {
        "title" : "User Attribute Name",
        "description" : "Name of the attribute which contains the user-ID. (property name:
org.forgerock.agents.user.mapping.mode.attribute.name) ",
        "propertyOrder" : 700,
        "type" : "object",
        "exampleValue" : "",
        "properties" : {
          "inherited" : {
            "type" : "boolean",
            "required" : true
          },
          "value" : {
            "type" : "string",
            "required" : false
          }
        }
      },
      "debugLogfileDirectory" : {
        "title" : "Debug Logfile Directory",
        "description" : "Location of the agent logs files, and where monitoring CSV files are
written. This is normally set in bootstrap properties during the install process. Note there is no
default and no logging will occur until a value for this property is provided. Anything logged will
be written to the standard output and may end up in the container log file (so \"catalina.out\" in
the case of Tomcat). (property: org.forgerock.agents.csv.monitoring.directory)",
        "propertyOrder" : 10060,
        "type" : "object",
        "exampleValue" : "",
        "properties" : {
```

```
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "debugLogfilePrefix" : {
          "title" : "Debug File Rotation Prefix",
          "description" : "Prefix which can be added onto the front of the debug file name when it is
rotated. (property: org.forgerock.agents.debug.prefix)",
          "propertyOrder" : 10010,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "localAuditLogfilePath" : {
          "title" : "Audit Logfile Path",
          "description" : "The full path of the local auditing file. (property:
org.forgerock.agents.local.audit.file.path)",
          "propertyOrder" : 2000,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "cdssoRootUrl" : {
          "title" : "Agent Root URL for CDSSO",
          "description" : "The agent root URL for CDSSO. The valid value is in the following format:
<br>protocol://hostname:port/<br> The protocol represents the protocol used, such as http or https.
The hostname represents the host name of the machine on which the agent resides. The port represents
the port number on which the agent is installed. The slash following the port number is required.",
          "propertyOrder" : 22700,
          "items" : {
            "type" : "string"
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
```

```
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "array",
              "required" : false
            }
          }
        },
        "filterMode" : {
          "title" : "Agent Filter Mode",
          "description" : "Specifies the mode of operation of the Filter. (property name:
org.forgerock.agents.filter.mode.map) <br>Valid key: the web application name. <br>Valid values:
ALL, URL_POLICY, SSO_ONLY, NONE <br>For this property, a global value can be set to apply to all
the applications that don't have their own specific filter mode. <br>Examples: <br>To set ALL as the
global filter mode: leave Map Key field empty, and enter ALL in Corresponding Map Value field. <br>To
set URL_POLICY as the filter mode for application BankApp: enter BankApp in Map Key field, and enter
URL_POLICY in Corresponding Map Value field.",
          "propertyOrder" : 500,
          "patternProperties" : {
            ".*" : {
              "type" : "string"
            }
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "object",
              "required" : false
            }
          }
        },
        "loginAttemptLimit" : {
          "title" : "Login Attempt Limit",
          "description" : "Limit of failed login attempts for a user's single browser session until
triggering the blocking of the user request. Value of 0 disables this feature. (property name:
org.forgerock.agents.login.attempt.limit.count) ",
          "propertyOrder" : 4400,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "integer",
              "required" : false
            }
          }
        },
        "debugLogfileRotationSize" : {
          "title" : "Debug File Rotation Size",
```

```
          "description" : "This specifies the approximate size in bytes at which a log file will be
rotated to a new log file. (property: org.forgerock.agents.debug.rotation.size.bytes)",
          "propertyOrder" : 10030,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "integer",
              "required" : false
            }
          }
        },
        "fallforwardModeEnabled" : {
          "title" : "Fall-Forward Mode",
          "description" : "This property is used when AM is not available. <br>  Disabled: the
Agent will deny every incoming request with an HTTP 403 <br>  Enabled: the Agent will continue
to allow access to any resource matched by a not enforced rule until AM becomes available again
<br><br>(property: org.forgerock.agents.session.change.notifications.enabled) (Agent 5.7+ only)",
          "propertyOrder" : 12115,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : false
            }
          }
        },
        "userPrincipalFlag" : {
          "title" : "User Principal Flag",
          "description" : "Use principal instead of just the user-ID for authenticating the user.
(property name: org.forgerock.agents.userid.mapping.mode.use.dn.enabled) ",
          "propertyOrder" : 800,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : false
            }
          }
        },
        "debugLogfileSuffix" : {
          "title" : "Debug File Rotation Suffix",
          "description" : "This is a value appended onto the end of the debug file name when it is
rotated. The user is free to define it as they want, but if it does not involve a timestamp that
```

```
produces different file names when the rotation time is reached, log file rotation is unlikely to
function correctly (property: org.forgerock.agents.debug.suffix)",
         "propertyOrder" : 10020,
         "type" : "object",
         "exampleValue" : "",
         "properties" : {
           "inherited" : {
             "type" : "boolean",
             "required" : true
           },
           "value" : {
             "type" : "string",
             "required" : false
           }
         }
       },
       "auditLogLocation" : {
         "title" : "Audit Log Location",
         "description" : "LOCAL = audit information stored in files based locally
to the Agent container <br>REMOTE = audit information logged via AM. (property name:
org.forgerock.agents.audit.where) ",
         "propertyOrder" : 1600,
         "type" : "object",
         "exampleValue" : "",
         "properties" : {
           "inherited" : {
             "type" : "boolean",
             "required" : true
           },
           "value" : {
             "type" : "string",
             "required" : false
           }
         }
       }
     }
   },
   "amServicesJ2EEAgent" : {
     "type" : "object",
     "title" : "AM Services",
     "propertyOrder" : 3,
     "properties" : {
       "urlPolicyEnvJsessionParameters" : {
         "title" : "URL Policy Env jsession Parameters",
         "description" : "List of HTTP SESSION attributes whose names and values will
be set in the environment map for URL policy evaluation at AM server. (property name:
org.forgerock.agents.continuous.security.http.session.list)  <br> Examples: <br> name <br>
phonenumber",
         "propertyOrder" : 12000,
         "items" : {
           "type" : "string"
         },
         "type" : "object",
         "exampleValue" : "",
         "properties" : {
           "inherited" : {
             "type" : "boolean",
             "required" : true
           },
```

```
            "value" : {
              "type" : "array",
              "required" : false
            }
          }
        },
        "conditionalLoginUrl" : {
          "title" : "AM Conditional Login URL",
          "description" : "(property name: org.forgerock.openam.agents.config.conditional.login.url)
  <br> Examples: <br> match|url?param1=value1&amp;ampparam2=value2 <br> match/path|?
param1=value1&amp;ampparam2=value2&amp;ampparam3=value3",
          "propertyOrder" : 3800,
          "items" : {
            "type" : "string"
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "array",
              "required" : false
            }
          }
        },
        "authSuccessRedirectUrl" : {
          "title" : "Redirect to AM's Success URL",
          "description" : "When enabled, the Agent will redirect to the session's Success URL instead
 (defined in auth. chain) of the originally requested resource after successful authentication.
 (property: org.forgerock.agents.authn.success.redirect.session.url.enabled)",
          "propertyOrder" : 4000,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : false
            }
          }
        },
        "agentAdviceEncode" : {
          "title" : "Composite Advice Encode",
          "description" : "This property is used to specify whether AM composite advices
 should be based64url encoded before sending to custom login endpoints. (property:
 org.forgerock.agents.advice.b64.url.encode)",
          "propertyOrder" : 13050,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
```

```
            },
            "value" : {
              "type" : "boolean",
              "required" : false
            }
          }
        },
        "policyEvaluationRealm" : {
          "title" : "Policy Evaluation Realm",
          "description" : "Which realm to start evaluating from. (property name:
org.forgerock.agents.policy.evaluation.realm.map) ",
          "propertyOrder" : 5400,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "authServicePort" : {
          "title" : "AM Authentication Service Port",
          "description" : "Port to be used by the AM authentication service. This property need
to be updated in OpenSSOAgentBootstrap.properties (property name: org.forgerock.agents.am.port)
<br>Required Agent Restart",
          "propertyOrder" : 11100,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "integer",
              "required" : false
            }
          }
        },
        "customLoginEnabled" : {
          "title" : "Allow Custom Login Mode",
          "description" : "Flag to enable custom login. (property:
org.forgerock.agents.legacy.login.enabled)",
          "propertyOrder" : 3700,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : false
```

```
            }
          }
        },
        "urlPolicyEnvPostParameters" : {
          "title" : "URL Policy Env POST Parameters",
          "description" : "List of HTTP POST request parameters whose names and values
will be set in the environment map for URL policy evaluation at AM server. (property name:
org.forgerock.agents.continuous.security.post.list)  <br> Examples: <br> name <br> phonenumber",
          "propertyOrder" : 11900,
          "items" : {
            "type" : "string"
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "array",
              "required" : false
            }
          }
        },
        "policyEvaluationApplication" : {
          "title" : "Policy Set",
          "description" : "Which application contains the policies to evaluate with. (property name:
org.forgerock.agents.policy.set.map) ",
          "propertyOrder" : 5500,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "urlPolicyEnvGetParameters" : {
          "title" : "URL Policy Env GET Parameters",
          "description" : "List of HTTP GET request parameters whose names and values will
be set in the environment map for URL policy evaluation at AM server. (property name:
org.forgerock.agents.continuous.security.get.list)  <br> Examples: <br> name <br> phonenumber",
          "propertyOrder" : 11800,
          "items" : {
            "type" : "string"
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
```

```
            "value" : {
              "type" : "array",
              "required" : false
            }
          }
        },
        "legacyLoginUrlList" : {
          "title" : "Custom Conditional Login URL",
          "description" : "Conditionally redirect users based on the incoming request URL.
 If the incoming request URL matches a specified domain name, the Java agent redirects
 the request to a specific URL. Conditional redirects have the format [Domain/path]|
[URL?realm=value&amp;amp;parameter1=value1...], with no spaces between values. <br>Example:
 myapp.domain.com|https://login.example.com/apps/login.jsp?realm=sales  <br>(property:
 org.forgerock.openam.agents.config.conditional.custom.login.url)",
          "propertyOrder" : 3900,
          "items" : {
            "type" : "string"
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "array",
              "required" : false
            }
          }
        },
        "authServiceProtocol" : {
          "title" : "AM Authentication Service Protocol",
          "description" : "Protocol to be used by the AM authentication service. This property need
 to be updated in OpenSSOAgentBootstrap.properties (property name: org.forgerock.agents.am.protocol)
 <br>Required Agent Restart",
          "propertyOrder" : 10900,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "policyNotifications" : {
          "title" : "Enable Policy Notifications",
          "description" : "Enable Notifications(via websockets) for remote policy client. (property
 name: org.forgerock.agents.policy.change.notifications.enabled) <br>Required Agent Restart",
          "propertyOrder" : 11200,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
```

```
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : false
            }
          }
        },
        "amLoginUrl" : {
          "title" : "AM Login URL",
          "description" : "AM login page URL. (property name:
com.sun.identity.agents.config.login.url)  <br> Example: <br> http://host:port/am/UI/Login",
          "propertyOrder" : 3710,
          "items" : {
            "type" : "string"
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "array",
              "required" : false
            }
          }
        },
        "restrictToRealm" : {
          "title" : "Restrict To Realm",
          "description" : "A map keyed by application name which allows users from only the
specified realms (each entry is a CSV) to access the specified application. If no restricted
realm is set, any user from any realm will be allowed access. Keyed by application name,
value is a comma separated list of realms from which users may request resources. (property:
org.forgerock.agents.restrict.to.realm.map)",
          "propertyOrder" : 13080,
          "patternProperties" : {
            ".*" : {
              "type" : "string"
            }
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "object",
              "required" : false
            }
          }
        },
        "authServiceHost" : {
          "title" : "AM Authentication Service Host Name",
```

```
          "description" : "Host name to be used by the AM authentication service. This property need
 to be updated in OpenSSOAgentBootstrap.properties (property name: org.forgerock.agents.am.hostname)
 <br>Required Agent Restart",
          "propertyOrder" : 11000,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "conditionalLogoutUrl" : {
          "title" : "AM Conditional Logout URL",
          "description" : "(property name: org.forgerock.agents.conditional.logout.url.list)
  <br> Examples: <br> match|url?param1=value1&amp;param2=value2 <br> match/path|?
param1=value1&amp;param2=value2&amp;param3=value3",
          "propertyOrder" : 12550,
          "items" : {
            "type" : "string"
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "array",
              "required" : false
            }
          }
        }
      }
    }
  }
}
```

JSONStdout

Realm Operations

Resource path: `/realm-config/services/audit/JSONStdout`

Resource version: `1.0`

create

Usage:

```
am> create JSONStdout --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "commonHandler" : {
      "type" : "object",
      "title" : "General Handler Configuration",
      "propertyOrder" : 0,
      "properties" : {
        "enabled" : {
          "title" : "Enabled",
          "description" : "Enables or disables an audit event handler.",
          "propertyOrder" : 300,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "topics" : {
          "title" : "Topics",
          "description" : "List of topics handled by an audit event handler.",
          "propertyOrder" : 400,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        }
      }
    },
    "jsonConfig" : {
      "type" : "object",
      "title" : "JSON Configuration",
      "propertyOrder" : 2,
      "properties" : {
        "elasticsearchCompatible" : {
          "title" : "ElasticSearch JSON Format Compatible",
          "description" : "JSON format should be transformed to be compatible with  ElasticSearch
 format restrictions.",
          "propertyOrder" : 1700,
          "required" : true,
```

```
          "type" : "boolean",
          "exampleValue" : ""
        }
      }
    },
    "commonHandlerPlugin" : {
      "type" : "object",
      "title" : "Audit Event Handler Factory",
      "propertyOrder" : 1,
      "properties" : {
        "handlerFactory" : {
          "title" : "Factory Class Name",
          "description" : "The fully qualified class name of the factory
 responsible for creating the Audit Event Handler. The class must implement
 <code>org.forgerock.openam.audit.AuditEventHandlerFactory</code>.",
          "propertyOrder" : 1900,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    }
  }
}
```

delete

Usage:

```
am> delete JSONStdout --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action JSONStdout --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action JSONStdout --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action JSONStdout --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query JSONStdout --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read JSONStdout --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update JSONStdout --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "commonHandler" : {
      "type" : "object",
      "title" : "General Handler Configuration",
      "propertyOrder" : 0,
      "properties" : {
        "enabled" : {
          "title" : "Enabled",
          "description" : "Enables or disables an audit event handler.",
          "propertyOrder" : 300,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "topics" : {
          "title" : "Topics",
          "description" : "List of topics handled by an audit event handler.",
          "propertyOrder" : 400,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        }
      }
    },
    "jsonConfig" : {
      "type" : "object",
      "title" : "JSON Configuration",
      "propertyOrder" : 2,
      "properties" : {
        "elasticsearchCompatible" : {
          "title" : "ElasticSearch JSON Format Compatible",
          "description" : "JSON format should be transformed to be compatible with  ElasticSearch
format restrictions.",
          "propertyOrder" : 1700,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        }
      }
    },
    "commonHandlerPlugin" : {
      "type" : "object",
      "title" : "Audit Event Handler Factory",
      "propertyOrder" : 1,
      "properties" : {
        "handlerFactory" : {
          "title" : "Factory Class Name",
          "description" : "The fully qualified class name of the factory
responsible for creating the Audit Event Handler. The class must implement
<code>org.forgerock.openam.audit.AuditEventHandlerFactory</code>.",
```

```
          "propertyOrder" : 1900,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    }
  }
}
```

Global Operations

Resource path: `/global-config/services/audit/JSONStdout`

Resource version: `1.0`

create

Usage:

```
am> create JSONStdout --global --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "commonHandler" : {
      "type" : "object",
      "title" : "General Handler Configuration",
      "propertyOrder" : 0,
      "properties" : {
        "enabled" : {
          "title" : "Enabled",
          "description" : "Enables or disables an audit event handler.",
          "propertyOrder" : 300,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "topics" : {
          "title" : "Topics",
          "description" : "List of topics handled by an audit event handler.",
          "propertyOrder" : 400,
          "required" : true,
```

```
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        }
      }
    },
    "jsonConfig" : {
      "type" : "object",
      "title" : "JSON Configuration",
      "propertyOrder" : 2,
      "properties" : {
        "elasticsearchCompatible" : {
          "title" : "ElasticSearch JSON Format Compatible",
          "description" : "JSON format should be transformed to be compatible with  ElasticSearch
 format restrictions.",
          "propertyOrder" : 1700,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        }
      }
    },
    "commonHandlerPlugin" : {
      "type" : "object",
      "title" : "Audit Event Handler Factory",
      "propertyOrder" : 1,
      "properties" : {
        "handlerFactory" : {
          "title" : "Factory Class Name",
          "description" : "The fully qualified class name of the factory
 responsible for creating the Audit Event Handler. The class must implement
 <code>org.forgerock.openam.audit.AuditEventHandlerFactory</code>.",
          "propertyOrder" : 1900,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    }
  }
}
```

delete

Usage:

```
am> delete JSONStdout --global --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action JSONStdout --global --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action JSONStdout --global --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action JSONStdout --global --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query JSONStdout --global --filter filter
```

Parameters:

`--filter`

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read JSONStdout --global --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update JSONStdout --global --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "commonHandler" : {
      "type" : "object",
      "title" : "General Handler Configuration",
      "propertyOrder" : 0,
      "properties" : {
        "enabled" : {
          "title" : "Enabled",
          "description" : "Enables or disables an audit event handler.",
          "propertyOrder" : 300,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "topics" : {
          "title" : "Topics",
          "description" : "List of topics handled by an audit event handler.",
          "propertyOrder" : 400,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        }
      }
    },
    "jsonConfig" : {
      "type" : "object",
      "title" : "JSON Configuration",
      "propertyOrder" : 2,
      "properties" : {
        "elasticsearchCompatible" : {
```

```
          "title" : "ElasticSearch JSON Format Compatible",
          "description" : "JSON format should be transformed to be compatible with  ElasticSearch
 format restrictions.",
          "propertyOrder" : 1700,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        }
      }
    },
    "commonHandlerPlugin" : {
      "type" : "object",
      "title" : "Audit Event Handler Factory",
      "propertyOrder" : 1,
      "properties" : {
        "handlerFactory" : {
          "title" : "Factory Class Name",
          "description" : "The fully qualified class name of the factory
 responsible for creating the Audit Event Handler. The class must implement
 <code>org.forgerock.openam.audit.AuditEventHandlerFactory</code>.",
          "propertyOrder" : 1900,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    }
  }
}
```

Jdbc

Realm Operations

Resource path: `/realm-config/services/audit/JDBC`

Resource version: `1.0`

create

Usage:

```
am> create Jdbc --realm Realm --id id --body body
```

Parameters:

`--id`

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "jdbcBuffering" : {
      "type" : "object",
      "title" : "Buffering",
      "propertyOrder" : 3,
      "properties" : {
        "bufferingMaxSize" : {
          "title" : "Buffer Size (number of events)",
          "description" : "Size of the queue where events are buffered before they are written to
 the database.<br><br>This queue has to be big enough to store all incoming events that have not yet
 been written to the database.<p>If the queue reaches capacity, the process will block until a write
 occurs.",
          "propertyOrder" : 4400,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "bufferingWriterThreads" : {
          "title" : "Writer Threads",
          "description" : "Specifies the number of threads used to write the buffered events.",
          "propertyOrder" : 4600,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "bufferingEnabled" : {
          "title" : "Buffering Enabled",
          "description" : "Enables or disables audit event buffering.",
          "propertyOrder" : 4300,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "bufferingMaxBatchedEvents" : {
          "title" : "Max Batched Events",
          "description" : "Specifies the maximum number of batched statements the database can support
 per connection.",
          "propertyOrder" : 4700,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "bufferingWriteInterval" : {
          "title" : "Write Interval",
          "description" : "Specifies the interval (seconds) at which buffered events are written to
 the database.",
          "propertyOrder" : 4500,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
```

```
    "commonHandler" : {
      "type" : "object",
      "title" : "General Handler Configuration",
      "propertyOrder" : 0,
      "properties" : {
        "enabled" : {
          "title" : "Enabled",
          "description" : "Enables or disables an audit event handler.",
          "propertyOrder" : 3100,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "topics" : {
          "title" : "Topics",
          "description" : "List of topics handled by an audit event handler.",
          "propertyOrder" : 3200,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        }
      }
    },
    "jdbcDatabaseConfig" : {
      "type" : "object",
      "title" : "Database Configuration",
      "propertyOrder" : 2,
      "properties" : {
        "connectionTimeout" : {
          "title" : "Connection Timeout (seconds)",
          "description" : "Specifies the maximum wait time before failing the connection, in
seconds.",
          "propertyOrder" : 3800,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "maxPoolSize" : {
          "title" : "Maximum Connections",
          "description" : "Specifies the maximum number of connections in the connection pool.",
          "propertyOrder" : 4200,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "username" : {
          "title" : "Database Username",
          "description" : "Specifies the username to access the database server.",
          "propertyOrder" : 3600,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "maxLifetime" : {
          "title" : "Maximum Connection Time (seconds)",
          "description" : "Specifies the maximum time a JDBC connection can be open, in seconds.",
```

```
          "propertyOrder" : 4000,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "idleTimeout" : {
          "title" : "Maximum Connection Idle Timeout (seconds)",
          "description" : "Specifies the maximum idle time before the connection is closed, in
seconds.",
          "propertyOrder" : 3900,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "password" : {
          "title" : "Database Password",
          "description" : "Specifies the password to access the database server.",
          "propertyOrder" : 3700,
          "required" : true,
          "type" : "string",
          "format" : "password",
          "exampleValue" : ""
        },
        "databaseType" : {
          "title" : "Database Type",
          "description" : "Select the database to use for logging audit events.<br><br>Identifies the
database in use, for example MySQL, Oracle, or SQL.",
          "propertyOrder" : 3300,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "jdbcUrl" : {
          "title" : "JDBC Database URL",
          "description" : "URL of the JDBC database.",
          "propertyOrder" : 3400,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "minIdle" : {
          "title" : "Minimum Idle Connections",
          "description" : "Specifies the minimum number of idle connections in the connection pool.",
          "propertyOrder" : 4100,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "driverClassName" : {
          "title" : "JDBC Driver",
          "description" : "Fully qualified JDBC driver class name.",
          "propertyOrder" : 3500,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "commonHandlerPlugin" : {
```

```
      "type" : "object",
      "title" : "Audit Event Handler Factory",
      "propertyOrder" : 1,
      "properties" : {
        "handlerFactory" : {
          "title" : "Factory Class Name",
          "description" : "The fully qualified class name of the factory
 responsible for creating the Audit Event Handler. The class must implement
 <code>org.forgerock.openam.audit.AuditEventHandlerFactory</code>.",
          "propertyOrder" : 4800,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    }
  }
}
```

delete

Usage:

```
am> delete Jdbc --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action Jdbc --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action Jdbc --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action Jdbc --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query Jdbc --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read Jdbc --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update Jdbc --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "jdbcBuffering" : {
      "type" : "object",
      "title" : "Buffering",
      "propertyOrder" : 3,
      "properties" : {
```

```
       "bufferingMaxSize" : {
         "title" : "Buffer Size (number of events)",
         "description" : "Size of the queue where events are buffered before they are written to
the database.<br><br>This queue has to be big enough to store all incoming events that have not yet
been written to the database.<p>If the queue reaches capacity, the process will block until a write
occurs.",
         "propertyOrder" : 4400,
         "required" : true,
         "type" : "string",
         "exampleValue" : ""
       },
       "bufferingWriterThreads" : {
         "title" : "Writer Threads",
         "description" : "Specifies the number of threads used to write the buffered events.",
         "propertyOrder" : 4600,
         "required" : true,
         "type" : "string",
         "exampleValue" : ""
       },
       "bufferingEnabled" : {
         "title" : "Buffering Enabled",
         "description" : "Enables or disables audit event buffering.",
         "propertyOrder" : 4300,
         "required" : true,
         "type" : "boolean",
         "exampleValue" : ""
       },
       "bufferingMaxBatchedEvents" : {
         "title" : "Max Batched Events",
         "description" : "Specifies the maximum number of batched statements the database can support
per connection.",
         "propertyOrder" : 4700,
         "required" : true,
         "type" : "string",
         "exampleValue" : ""
       },
       "bufferingWriteInterval" : {
         "title" : "Write Interval",
         "description" : "Specifies the interval (seconds) at which buffered events are written to
the database.",
         "propertyOrder" : 4500,
         "required" : true,
         "type" : "string",
         "exampleValue" : ""
       }
     }
   },
   "commonHandler" : {
     "type" : "object",
     "title" : "General Handler Configuration",
     "propertyOrder" : 0,
     "properties" : {
       "enabled" : {
         "title" : "Enabled",
         "description" : "Enables or disables an audit event handler.",
         "propertyOrder" : 3100,
         "required" : true,
         "type" : "boolean",
         "exampleValue" : ""
```

```
       },
       "topics" : {
         "title" : "Topics",
         "description" : "List of topics handled by an audit event handler.",
         "propertyOrder" : 3200,
         "required" : true,
         "items" : {
           "type" : "string"
         },
         "type" : "array",
         "exampleValue" : ""
       }
     }
   },
   "jdbcDatabaseConfig" : {
     "type" : "object",
     "title" : "Database Configuration",
     "propertyOrder" : 2,
     "properties" : {
       "connectionTimeout" : {
         "title" : "Connection Timeout (seconds)",
         "description" : "Specifies the maximum wait time before failing the connection, in
seconds.",
         "propertyOrder" : 3800,
         "required" : true,
         "type" : "string",
         "exampleValue" : ""
       },
       "maxPoolSize" : {
         "title" : "Maximum Connections",
         "description" : "Specifies the maximum number of connections in the connection pool.",
         "propertyOrder" : 4200,
         "required" : true,
         "type" : "string",
         "exampleValue" : ""
       },
       "username" : {
         "title" : "Database Username",
         "description" : "Specifies the username to access the database server.",
         "propertyOrder" : 3600,
         "required" : true,
         "type" : "string",
         "exampleValue" : ""
       },
       "maxLifetime" : {
         "title" : "Maximum Connection Time (seconds)",
         "description" : "Specifies the maximum time a JDBC connection can be open, in seconds.",
         "propertyOrder" : 4000,
         "required" : true,
         "type" : "string",
         "exampleValue" : ""
       },
       "idleTimeout" : {
         "title" : "Maximum Connection Idle Timeout (seconds)",
         "description" : "Specifies the maximum idle time before the connection is closed, in
seconds.",
         "propertyOrder" : 3900,
         "required" : true,
         "type" : "string",
```

```
          "exampleValue" : ""
        },
        "password" : {
          "title" : "Database Password",
          "description" : "Specifies the password to access the database server.",
          "propertyOrder" : 3700,
          "required" : true,
          "type" : "string",
          "format" : "password",
          "exampleValue" : ""
        },
        "databaseType" : {
          "title" : "Database Type",
          "description" : "Select the database to use for logging audit events.<br><br>Identifies the
database in use, for example MySQL, Oracle, or SQL.",
          "propertyOrder" : 3300,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "jdbcUrl" : {
          "title" : "JDBC Database URL",
          "description" : "URL of the JDBC database.",
          "propertyOrder" : 3400,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "minIdle" : {
          "title" : "Minimum Idle Connections",
          "description" : "Specifies the minimum number of idle connections in the connection pool.",
          "propertyOrder" : 4100,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "driverClassName" : {
          "title" : "JDBC Driver",
          "description" : "Fully qualified JDBC driver class name.",
          "propertyOrder" : 3500,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "commonHandlerPlugin" : {
      "type" : "object",
      "title" : "Audit Event Handler Factory",
      "propertyOrder" : 1,
      "properties" : {
        "handlerFactory" : {
          "title" : "Factory Class Name",
          "description" : "The fully qualified class name of the factory
responsible for creating the Audit Event Handler. The class must implement
<code>org.forgerock.openam.audit.AuditEventHandlerFactory</code>.",
          "propertyOrder" : 4800,
          "required" : true,
          "type" : "string",
```

```
          "exampleValue" : ""
        }
      }
    }
  }
}
```

Global Operations

Resource path: `/global-config/services/audit/JDBC`

Resource version: `1.0`

create

Usage:

```
am> create Jdbc --global --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "jdbcBuffering" : {
      "type" : "object",
      "title" : "Buffering",
      "propertyOrder" : 3,
      "properties" : {
        "bufferingWriterThreads" : {
          "title" : "Writer Threads",
          "description" : "Specifies the number of threads used to write the buffered events.",
          "propertyOrder" : 4600,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "bufferingWriteInterval" : {
          "title" : "Write Interval",
          "description" : "Specifies the interval (seconds) at which buffered events are written to
 the database.",
          "propertyOrder" : 4500,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
```

```
       "bufferingMaxSize" : {
         "title" : "Buffer Size (number of events)",
         "description" : "Size of the queue where events are buffered before they are written to
the database.<br><br>This queue has to be big enough to store all incoming events that have not yet
been written to the database.<p>If the queue reaches capacity, the process will block until a write
occurs.",
         "propertyOrder" : 4400,
         "required" : true,
         "type" : "string",
         "exampleValue" : ""
       },
       "bufferingEnabled" : {
         "title" : "Buffering Enabled",
         "description" : "Enables or disables audit event buffering.",
         "propertyOrder" : 4300,
         "required" : true,
         "type" : "boolean",
         "exampleValue" : ""
       },
       "bufferingMaxBatchedEvents" : {
         "title" : "Max Batched Events",
         "description" : "Specifies the maximum number of batched statements the database can support
per connection.",
         "propertyOrder" : 4700,
         "required" : true,
         "type" : "string",
         "exampleValue" : ""
       }
     }
   },
   "jdbcDatabaseConfig" : {
     "type" : "object",
     "title" : "Database Configuration",
     "propertyOrder" : 2,
     "properties" : {
       "idleTimeout" : {
         "title" : "Maximum Connection Idle Timeout (seconds)",
         "description" : "Specifies the maximum idle time before the connection is closed, in
seconds.",
         "propertyOrder" : 3900,
         "required" : true,
         "type" : "string",
         "exampleValue" : ""
       },
       "username" : {
         "title" : "Database Username",
         "description" : "Specifies the username to access the database server.",
         "propertyOrder" : 3600,
         "required" : true,
         "type" : "string",
         "exampleValue" : ""
       },
       "databaseType" : {
         "title" : "Database Type",
         "description" : "Select the database to use for logging audit events.<br><br>Identifies the
database in use, for example MySQL, Oracle, or SQL.",
         "propertyOrder" : 3300,
         "required" : true,
         "type" : "string",
```

```
          "exampleValue" : ""
        },
        "connectionTimeout" : {
          "title" : "Connection Timeout (seconds)",
          "description" : "Specifies the maximum wait time before failing the connection, in
seconds.",
          "propertyOrder" : 3800,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "password" : {
          "title" : "Database Password",
          "description" : "Specifies the password to access the database server.",
          "propertyOrder" : 3700,
          "required" : true,
          "type" : "string",
          "format" : "password",
          "exampleValue" : ""
        },
        "driverClassName" : {
          "title" : "JDBC Driver",
          "description" : "Fully qualified JDBC driver class name.",
          "propertyOrder" : 3500,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "minIdle" : {
          "title" : "Minimum Idle Connections",
          "description" : "Specifies the minimum number of idle connections in the connection pool.",
          "propertyOrder" : 4100,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "maxPoolSize" : {
          "title" : "Maximum Connections",
          "description" : "Specifies the maximum number of connections in the connection pool.",
          "propertyOrder" : 4200,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "jdbcUrl" : {
          "title" : "JDBC Database URL",
          "description" : "URL of the JDBC database.",
          "propertyOrder" : 3400,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "maxLifetime" : {
          "title" : "Maximum Connection Time (seconds)",
          "description" : "Specifies the maximum time a JDBC connection can be open, in seconds.",
          "propertyOrder" : 4000,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
```

```
        }
      }
    },
    "commonHandlerPlugin" : {
      "type" : "object",
      "title" : "Audit Event Handler Factory",
      "propertyOrder" : 1,
      "properties" : {
        "handlerFactory" : {
          "title" : "Factory Class Name",
          "description" : "The fully qualified class name of the factory
 responsible for creating the Audit Event Handler. The class must implement
 <code>org.forgerock.openam.audit.AuditEventHandlerFactory</code>.",
          "propertyOrder" : 4800,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "commonHandler" : {
      "type" : "object",
      "title" : "General Handler Configuration",
      "propertyOrder" : 0,
      "properties" : {
        "enabled" : {
          "title" : "Enabled",
          "description" : "Enables or disables an audit event handler.",
          "propertyOrder" : 3100,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "topics" : {
          "title" : "Topics",
          "description" : "List of topics handled by an audit event handler.",
          "propertyOrder" : 3200,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        }
      }
    }
  }
}
```

delete

Usage:

```
am> delete Jdbc --global --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action Jdbc --global --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action Jdbc --global --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action Jdbc --global --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query Jdbc --global --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read Jdbc --global --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update Jdbc --global --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "jdbcBuffering" : {
      "type" : "object",
      "title" : "Buffering",
      "propertyOrder" : 3,
      "properties" : {
        "bufferingWriterThreads" : {
          "title" : "Writer Threads",
          "description" : "Specifies the number of threads used to write the buffered events.",
          "propertyOrder" : 4600,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "bufferingWriteInterval" : {
          "title" : "Write Interval",
          "description" : "Specifies the interval (seconds) at which buffered events are written to
the database.",
          "propertyOrder" : 4500,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "bufferingMaxSize" : {
          "title" : "Buffer Size (number of events)",
          "description" : "Size of the queue where events are buffered before they are written to
the database.<br><br>This queue has to be big enough to store all incoming events that have not yet
been written to the database.<p>If the queue reaches capacity, the process will block until a write
occurs.",
          "propertyOrder" : 4400,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
```

```
       "bufferingEnabled" : {
         "title" : "Buffering Enabled",
         "description" : "Enables or disables audit event buffering.",
         "propertyOrder" : 4300,
         "required" : true,
         "type" : "boolean",
         "exampleValue" : ""
       },
       "bufferingMaxBatchedEvents" : {
         "title" : "Max Batched Events",
         "description" : "Specifies the maximum number of batched statements the database can support
per connection.",
         "propertyOrder" : 4700,
         "required" : true,
         "type" : "string",
         "exampleValue" : ""
       }
     }
   },
   "jdbcDatabaseConfig" : {
     "type" : "object",
     "title" : "Database Configuration",
     "propertyOrder" : 2,
     "properties" : {
       "idleTimeout" : {
         "title" : "Maximum Connection Idle Timeout (seconds)",
         "description" : "Specifies the maximum idle time before the connection is closed, in
seconds.",
         "propertyOrder" : 3900,
         "required" : true,
         "type" : "string",
         "exampleValue" : ""
       },
       "username" : {
         "title" : "Database Username",
         "description" : "Specifies the username to access the database server.",
         "propertyOrder" : 3600,
         "required" : true,
         "type" : "string",
         "exampleValue" : ""
       },
       "databaseType" : {
         "title" : "Database Type",
         "description" : "Select the database to use for logging audit events.<br><br>Identifies the
database in use, for example MySQL, Oracle, or SQL.",
         "propertyOrder" : 3300,
         "required" : true,
         "type" : "string",
         "exampleValue" : ""
       },
       "connectionTimeout" : {
         "title" : "Connection Timeout (seconds)",
         "description" : "Specifies the maximum wait time before failing the connection, in
seconds.",
         "propertyOrder" : 3800,
         "required" : true,
         "type" : "string",
         "exampleValue" : ""
       },
```

```
        "password" : {
          "title" : "Database Password",
          "description" : "Specifies the password to access the database server.",
          "propertyOrder" : 3700,
          "required" : true,
          "type" : "string",
          "format" : "password",
          "exampleValue" : ""
        },
        "driverClassName" : {
          "title" : "JDBC Driver",
          "description" : "Fully qualified JDBC driver class name.",
          "propertyOrder" : 3500,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "minIdle" : {
          "title" : "Minimum Idle Connections",
          "description" : "Specifies the minimum number of idle connections in the connection pool.",
          "propertyOrder" : 4100,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "maxPoolSize" : {
          "title" : "Maximum Connections",
          "description" : "Specifies the maximum number of connections in the connection pool.",
          "propertyOrder" : 4200,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "jdbcUrl" : {
          "title" : "JDBC Database URL",
          "description" : "URL of the JDBC database.",
          "propertyOrder" : 3400,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "maxLifetime" : {
          "title" : "Maximum Connection Time (seconds)",
          "description" : "Specifies the maximum time a JDBC connection can be open, in seconds.",
          "propertyOrder" : 4000,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "commonHandlerPlugin" : {
      "type" : "object",
      "title" : "Audit Event Handler Factory",
      "propertyOrder" : 1,
      "properties" : {
        "handlerFactory" : {
          "title" : "Factory Class Name",
```

```
          "description" : "The fully qualified class name of the factory
 responsible for creating the Audit Event Handler. The class must implement
 <code>org.forgerock.openam.audit.AuditEventHandlerFactory</code>.",
          "propertyOrder" : 4800,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "commonHandler" : {
      "type" : "object",
      "title" : "General Handler Configuration",
      "propertyOrder" : 0,
      "properties" : {
        "enabled" : {
          "title" : "Enabled",
          "description" : "Enables or disables an audit event handler.",
          "propertyOrder" : 3100,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "topics" : {
          "title" : "Topics",
          "description" : "List of topics handled by an audit event handler.",
          "propertyOrder" : 3200,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        }
      }
    }
  }
}
```

JdbcModule

Realm Operations

Resource path: `/realm-config/authentication/modules/jdbc`

Resource version: `1.0`

create

Usage:

```
am> create JdbcModule --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "passwordStatement" : {
      "title" : "Prepared Statement",
      "description" : "The SQL statement used to search the database for user passwords<br><br>The
 SQL statement used to search the database for the user password. A single property of the supplied
 username is provided by the module. The result of the search should be a single row that contains the
 password for the user under the specified column.",
      "propertyOrder" : 800,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "passwordTransformClass" : {
      "title" : "Class to Transform Password Syntax",
      "description" : "This class is used to transform the supplied credentials from the
 database.<br><br>The default implementation for this property is <code>ClearTextTransform</
code> that performs no transformation. If the supplied credentials need to be transformed
 before comparing with the password field retrieved from the database, a custom implementation
 should be provided. Any custom implementation must implement the following interface
 <code>com.sun.identity.authentication.modules.jdbc.JDBCPasswordSyntaxTransform</code>",
      "propertyOrder" : 900,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "authenticationLevel" : {
      "title" : "Authentication Level",
      "description" : "The authentication level associated with this module.<br><br>Each
 authentication module has an authentication level that can be used to indicate the level of security
 associated with the module; 0 is the lowest (and the default).",
      "propertyOrder" : 1000,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "connectionType" : {
      "title" : "Connection Type",
      "description" : "Controls how the authentication module will obtain the JDBC connection to
 the database.<br><br>If the connection type is non-persistent JDBC connection then the JDBC driver
 must be available to the OpenAM web-app. If the connection type is JNDI, the OpenAM web application
 deployment descriptor <code>web.xml</code> must be updated to include the correct JNDI JDBC resource
 information. The J2EE container must also be configured with the correct JNDI JDBC configuration.",
      "propertyOrder" : 100,
      "required" : true,
```

```
      "type" : "string",
      "exampleValue" : ""
    },
    "jdbcDriver" : {
      "title" : "JDBC Driver",
      "description" : "The classname of the JDBC driver to use.<br><br>The fully qualified class name
 of the JDBC driver to use to connect to the database. Only Oracle or MySQL drivers are supported.
 JDBC drivers for other database may work, but the database will be treated as if it was Oracle.<br/
><br/><i>NB </i>Only used when connection type is JDBC",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "password" : {
      "title" : "Database Password",
      "description" : "The password used to authenticate to the database<br><br><i>NB </i>Only used
 when connection type is JDBC",
      "propertyOrder" : 600,
      "required" : true,
      "type" : "string",
      "format" : "password",
      "exampleValue" : ""
    },
    "username" : {
      "title" : "Database Username",
      "description" : "This username will be used to authenticate to the database<br><br><i>NB </
i>Only used when connection type is JDBC",
      "propertyOrder" : 500,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "connectionPoolJndiName" : {
      "title" : "Connection Pool JNDI Name",
      "description" : "The JNDI URL to the JDBC connection pool<br><br>The JNDI URL refers to the
 JDBC connection pool created in the J2EE container for the authentication database.<br/><br/><i>NB </
i>Only used when connection type is JNDI",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "passwordColumn" : {
      "title" : "Password Column Name",
      "description" : "The name of the column in the database containing the user
 passwords<br><br>This property will be used to retrieve the correct column containing the password
 from the results table returned by the database",
      "propertyOrder" : 700,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "jdbcUrl" : {
      "title" : "JDBC URL",
      "description" : "The JDBC URL used to initialise the JDBC driver<br><br><i>NB </i>Only used when
 connection type is JDBC",
      "propertyOrder" : 400,
      "required" : true,
```

```
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
```

delete

Usage:

```
am> delete JdbcModule --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action JdbcModule --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action JdbcModule --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action JdbcModule --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query JdbcModule --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read JdbcModule --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update JdbcModule --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "passwordStatement" : {
      "title" : "Prepared Statement",
      "description" : "The SQL statement used to search the database for user passwords<br><br>The
 SQL statement used to search the database for the user password. A single property of the supplied
 username is provided by the module. The result of the search should be a single row that contains the
 password for the user under the specified column.",
      "propertyOrder" : 800,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "passwordTransformClass" : {
      "title" : "Class to Transform Password Syntax",
      "description" : "This class is used to transform the supplied credentials from the
 database.<br><br>The default implementation for this property is <code>ClearTextTransform</
code> that performs no transformation. If the supplied credentials need to be transformed
 before comparing with the password field retrieved from the database, a custom implementation
```

```
 should be provided. Any custom implementation must implement the following interface
 <code>com.sun.identity.authentication.modules.jdbc.JDBCPasswordSyntaxTransform</code>",
      "propertyOrder" : 900,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "authenticationLevel" : {
      "title" : "Authentication Level",
      "description" : "The authentication level associated with this module.<br><br>Each
 authentication module has an authentication level that can be used to indicate the level of security
 associated with the module; 0 is the lowest (and the default).",
      "propertyOrder" : 1000,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "connectionType" : {
      "title" : "Connection Type",
      "description" : "Controls how the authentication module will obtain the JDBC connection to
 the database.<br><br>If the connection type is non-persistent JDBC connection then the JDBC driver
 must be available to the OpenAM web-app. If the connection type is JNDI, the OpenAM web application
 deployment descriptor <code>web.xml</code> must be updated to include the correct JNDI JDBC resource
 information. The J2EE container must also be configured with the correct JNDI JDBC configuration.",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "jdbcDriver" : {
      "title" : "JDBC Driver",
      "description" : "The classname of the JDBC driver to use.<br><br>The fully qualified class name
 of the JDBC driver to use to connect to the database. Only Oracle or MySQL drivers are supported.
 JDBC drivers for other database may work, but the database will be treated as if it was Oracle.<br/
><br/><i>NB </i>Only used when connection type is JDBC",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "password" : {
      "title" : "Database Password",
      "description" : "The password used to authenticate to the database<br><br><i>NB </i>Only used
 when connection type is JDBC",
      "propertyOrder" : 600,
      "required" : true,
      "type" : "string",
      "format" : "password",
      "exampleValue" : ""
    },
    "username" : {
      "title" : "Database Username",
      "description" : "This username will be used to authenticate to the database<br><br><i>NB </
i>Only used when connection type is JDBC",
      "propertyOrder" : 500,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
```

```
    "connectionPoolJndiName" : {
      "title" : "Connection Pool JNDI Name",
      "description" : "The JNDI URL to the JDBC connection pool<br><br>The JNDI URL refers to the
 JDBC connection pool created in the J2EE container for the authentication database.<br/><br/><i>NB </
i>Only used when connection type is JNDI",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "passwordColumn" : {
      "title" : "Password Column Name",
      "description" : "The name of the column in the database containing the user
 passwords<br><br>This property will be used to retrieve the correct column containing the password
 from the results table returned by the database",
      "propertyOrder" : 700,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "jdbcUrl" : {
      "title" : "JDBC URL",
      "description" : "The JDBC URL used to initialise the JDBC driver<br><br><i>NB </i>Only used when
 connection type is JDBC",
      "propertyOrder" : 400,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
```

Global Operations

Resource path: `/global-config/authentication/modules/jdbc`

Resource version: `1.0`

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action JdbcModule --global --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action JdbcModule --global --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action JdbcModule --global --actionName nextdescendents
```

read

Usage:

```
am> read JdbcModule --global
```

update

Usage:

```
am> update JdbcModule --global --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "defaults" : {
      "properties" : {
        "connectionPoolJndiName" : {
          "title" : "Connection Pool JNDI Name",
          "description" : "The JNDI URL to the JDBC connection pool<br><br>The JNDI URL refers to the
 JDBC connection pool created in the J2EE container for the authentication database.<br/><br/><i>NB </
i>Only used when connection type is JNDI",
          "propertyOrder" : 200,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "connectionType" : {
          "title" : "Connection Type",
          "description" : "Controls how the authentication module will obtain the JDBC connection to
 the database.<br><br>If the connection type is non-persistent JDBC connection then the JDBC driver
 must be available to the OpenAM web-app. If the connection type is JNDI, the OpenAM web application
 deployment descriptor <code>web.xml</code> must be updated to include the correct JNDI JDBC resource
 information. The J2EE container must also be configured with the correct JNDI JDBC configuration.",
          "propertyOrder" : 100,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "passwordTransformClass" : {
```

```
          "title" : "Class to Transform Password Syntax",
          "description" : "This class is used to transform the supplied credentials from the
 database.<br><br>The default implementation for this property is <code>ClearTextTransform</
code> that performs no transformation. If the supplied credentials need to be transformed
 before comparing with the password field retrieved from the database, a custom implementation
 should be provided. Any custom implementation must implement the following interface
 <code>com.sun.identity.authentication.modules.jdbc.JDBCPasswordSyntaxTransform</code>",
          "propertyOrder" : 900,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "username" : {
          "title" : "Database Username",
          "description" : "This username will be used to authenticate to the database<br><br><i>NB </
i>Only used when connection type is JDBC",
          "propertyOrder" : 500,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "passwordStatement" : {
          "title" : "Prepared Statement",
          "description" : "The SQL statement used to search the database for user passwords<br><br>The
 SQL statement used to search the database for the user password. A single property of the supplied
 username is provided by the module. The result of the search should be a single row that contains the
 password for the user under the specified column.",
          "propertyOrder" : 800,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "passwordColumn" : {
          "title" : "Password Column Name",
          "description" : "The name of the column in the database containing the user
 passwords<br><br>This property will be used to retrieve the correct column containing the password
 from the results table returned by the database",
          "propertyOrder" : 700,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "password" : {
          "title" : "Database Password",
          "description" : "The password used to authenticate to the database<br><br><i>NB </i>Only
 used when connection type is JDBC",
          "propertyOrder" : 600,
          "required" : true,
          "type" : "string",
          "format" : "password",
          "exampleValue" : ""
        },
        "jdbcUrl" : {
          "title" : "JDBC URL",
          "description" : "The JDBC URL used to initialise the JDBC driver<br><br><i>NB </i>Only used
 when connection type is JDBC",
          "propertyOrder" : 400,
          "required" : true,
          "type" : "string",
```

```
          "exampleValue" : ""
        },
        "jdbcDriver" : {
          "title" : "JDBC Driver",
          "description" : "The classname of the JDBC driver to use.<br><br>The fully qualified
 class name of the JDBC driver to use to connect to the database. Only Oracle or MySQL drivers are
 supported. JDBC drivers for other database may work, but the database will be treated as if it was
 Oracle.<br/><br/><i>NB </i>Only used when connection type is JDBC",
          "propertyOrder" : 300,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "authenticationLevel" : {
          "title" : "Authentication Level",
          "description" : "The authentication level associated with this module.<br><br>Each
 authentication module has an authentication level that can be used to indicate the level of security
 associated with the module; 0 is the lowest (and the default).",
          "propertyOrder" : 1000,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        }
      },
      "type" : "object",
      "title" : "Realm Defaults"
    }
  }
}
```


Jms

Realm Operations

Resource path: `/realm-config/services/audit/JMS`

Resource version: `1.0`

create

Usage:

```
am> create Jms --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "jmsConfiguration" : {
      "type" : "object",
      "title" : "JMS Configuration",
      "propertyOrder" : 2,
      "properties" : {
        "deliveryMode" : {
          "title" : "Delivery Mode",
          "description" : "Specifies whether JMS messages used to transmit audit events use persistent
or non-persistent delivery.<p><p>With persistent delivery, the JMS provider ensures that messages
are not lost in transit in case of a provider failure by logging messages to storage when they are
sent.<p>Specify the delivery mode as persistent if it is unacceptable for delivery of audit events
to be lost in JMS transit. If the possible loss of audit events is acceptable, choose non-persistent
delivery, which provides better performance.",
          "propertyOrder" : 6400,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "jndiConnectionFactoryName" : {
          "title" : "JMS Connection Factory Name",
          "description" : "Specifies the JNDI lookup name for the connection factory exposed by your
JMS message broker. OpenAM performs a JNDI lookup on this name to locate your broker's connection
factory.<p><p>See the documentation for your JMS message broker for the required value.<p>The default
is the connection factory name for Apache ActiveMQ.",
          "propertyOrder" : 6800,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "jndiContextProperties" : {
          "title" : "JNDI Context Properties",
          "description" : "Specifies JNDI properties that OpenAM uses to connect to the JMS message
broker to which OpenAM will publish audit events.<p><p>OpenAM acts as a JMS client, using a JMS
connection factory to connect to your JMS message broker. In order for OpenAM to connect to the
broker, the JNDI context properties must conform to those needed by the broker. See the documentation
for your JMS message broker for required values.<p>The default properties are example properties for
connecting to Apache ActiveMQ.",
          "propertyOrder" : 6600,
          "required" : true,
          "patternProperties" : {
            ".*" : {
              "type" : "string"
            }
          },
          "type" : "object",
          "exampleValue" : ""
        },
        "jndiTopicName" : {
          "title" : "JMS Topic Name",
          "description" : "JNDI lookup name for the JMS topic",
          "propertyOrder" : 6700,
          "required" : true,
```

```
          "type" : "string",
          "exampleValue" : ""
        },
        "sessionMode" : {
          "title" : "Session Mode",
          "description" : "Specifies the JMS session acknowledgement mode: <code>AUTO</code>,
<code>CLIENT</code>, or <code>DUPS_OK</code>.<p><ul><li>Auto mode guarantees once-only delivery of
JMS messages used to transmit audit events.</li><li>Duplicates OK mode ensures that messages are
delivered at least once.</li><li>Client mode does not ensure delivery.</li></ul><p>Use the default
setting unless your JMS broker implementation requires otherwise. See your broker documentation for
more information.",
          "propertyOrder" : 6500,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "batchEvents" : {
      "type" : "object",
      "title" : "Batch Events",
      "propertyOrder" : 3,
      "properties" : {
        "batchCapacity" : {
          "title" : "Capacity",
          "description" : "Maximum event count in the batch queue; additional events are dropped.",
          "propertyOrder" : 7000,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "maxBatchedEvents" : {
          "title" : "Max Batched",
          "description" : "Maximum number of events per batch.",
          "propertyOrder" : 7100,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "pollTimeoutSec" : {
          "title" : "Writing Interval",
          "description" : "The interval (in seconds) for reading events from the buffer to transmit
via jms.",
          "propertyOrder" : 7400,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        }
      }
    },
    "commonHandler" : {
      "type" : "object",
      "title" : "General Handler Configuration",
      "propertyOrder" : 0,
      "properties" : {
        "enabled" : {
          "title" : "Enabled",
          "description" : "Enables or disables an audit event handler.",
          "propertyOrder" : 6200,
```

```
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "topics" : {
          "title" : "Topics",
          "description" : "List of topics handled by an audit event handler.",
          "propertyOrder" : 6300,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        }
      }
    },
    "commonHandlerPlugin" : {
      "type" : "object",
      "title" : "Audit Event Handler Factory",
      "propertyOrder" : 1,
      "properties" : {
        "handlerFactory" : {
          "title" : "Factory Class Name",
          "description" : "The fully qualified class name of the factory
 responsible for creating the Audit Event Handler. The class must implement
 <code>org.forgerock.openam.audit.AuditEventHandlerFactory</code>.",
          "propertyOrder" : 7600,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    }
  }
}
```

delete

Usage:

```
am> delete Jms --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action Jms --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action Jms --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action Jms --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query Jms --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read Jms --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update Jms --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "jmsConfiguration" : {
      "type" : "object",
      "title" : "JMS Configuration",
      "propertyOrder" : 2,
      "properties" : {
        "deliveryMode" : {
          "title" : "Delivery Mode",
          "description" : "Specifies whether JMS messages used to transmit audit events use persistent
or non-persistent delivery.<p><p>With persistent delivery, the JMS provider ensures that messages
are not lost in transit in case of a provider failure by logging messages to storage when they are
sent.<p>Specify the delivery mode as persistent if it is unacceptable for delivery of audit events
to be lost in JMS transit. If the possible loss of audit events is acceptable, choose non-persistent
delivery, which provides better performance.",
          "propertyOrder" : 6400,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "jndiConnectionFactoryName" : {
          "title" : "JMS Connection Factory Name",
          "description" : "Specifies the JNDI lookup name for the connection factory exposed by your
JMS message broker. OpenAM performs a JNDI lookup on this name to locate your broker's connection
factory.<p><p>See the documentation for your JMS message broker for the required value.<p>The default
is the connection factory name for Apache ActiveMQ.",
          "propertyOrder" : 6800,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "jndiContextProperties" : {
          "title" : "JNDI Context Properties",
          "description" : "Specifies JNDI properties that OpenAM uses to connect to the JMS message
broker to which OpenAM will publish audit events.<p><p>OpenAM acts as a JMS client, using a JMS
connection factory to connect to your JMS message broker. In order for OpenAM to connect to the
broker, the JNDI context properties must conform to those needed by the broker. See the documentation
for your JMS message broker for required values.<p>The default properties are example properties for
connecting to Apache ActiveMQ.",
          "propertyOrder" : 6600,
          "required" : true,
          "patternProperties" : {
            ".*" : {
              "type" : "string"
            }
          },
          "type" : "object",
          "exampleValue" : ""
```

```
       },
       "jndiTopicName" : {
         "title" : "JMS Topic Name",
         "description" : "JNDI lookup name for the JMS topic",
         "propertyOrder" : 6700,
         "required" : true,
         "type" : "string",
         "exampleValue" : ""
       },
       "sessionMode" : {
         "title" : "Session Mode",
         "description" : "Specifies the JMS session acknowledgement mode: <code>AUTO</code>,
<code>CLIENT</code>, or <code>DUPS_OK</code>.<p><ul><li>Auto mode guarantees once-only delivery of
JMS messages used to transmit audit events.</li><li>Duplicates OK mode ensures that messages are
delivered at least once.</li><li>Client mode does not ensure delivery.</li></ul><p>Use the default
setting unless your JMS broker implementation requires otherwise. See your broker documentation for
more information.",
         "propertyOrder" : 6500,
         "required" : true,
         "type" : "string",
         "exampleValue" : ""
       }
     }
   },
   "batchEvents" : {
     "type" : "object",
     "title" : "Batch Events",
     "propertyOrder" : 3,
     "properties" : {
       "batchCapacity" : {
         "title" : "Capacity",
         "description" : "Maximum event count in the batch queue; additional events are dropped.",
         "propertyOrder" : 7000,
         "required" : true,
         "type" : "integer",
         "exampleValue" : ""
       },
       "maxBatchedEvents" : {
         "title" : "Max Batched",
         "description" : "Maximum number of events per batch.",
         "propertyOrder" : 7100,
         "required" : true,
         "type" : "integer",
         "exampleValue" : ""
       },
       "pollTimeoutSec" : {
         "title" : "Writing Interval",
         "description" : "The interval (in seconds) for reading events from the buffer to transmit
via jms.",
         "propertyOrder" : 7400,
         "required" : true,
         "type" : "integer",
         "exampleValue" : ""
       }
     }
   },
   "commonHandler" : {
     "type" : "object",
     "title" : "General Handler Configuration",
```

```
      "propertyOrder" : 0,
      "properties" : {
        "enabled" : {
          "title" : "Enabled",
          "description" : "Enables or disables an audit event handler.",
          "propertyOrder" : 6200,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "topics" : {
          "title" : "Topics",
          "description" : "List of topics handled by an audit event handler.",
          "propertyOrder" : 6300,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        }
      }
    },
    "commonHandlerPlugin" : {
      "type" : "object",
      "title" : "Audit Event Handler Factory",
      "propertyOrder" : 1,
      "properties" : {
        "handlerFactory" : {
          "title" : "Factory Class Name",
          "description" : "The fully qualified class name of the factory
 responsible for creating the Audit Event Handler. The class must implement
 <code>org.forgerock.openam.audit.AuditEventHandlerFactory</code>.",
          "propertyOrder" : 7600,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    }
  }
}
```

Global Operations

Resource path: `/global-config/services/audit/JMS`

Resource version: `1.0`

create

Usage:

```
am> create Jms --global --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "batchEvents" : {
      "type" : "object",
      "title" : "Batch Events",
      "propertyOrder" : 3,
      "properties" : {
        "batchCapacity" : {
          "title" : "Capacity",
          "description" : "Maximum event count in the batch queue; additional events are dropped.",
          "propertyOrder" : 7000,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "pollTimeoutSec" : {
          "title" : "Writing Interval",
          "description" : "The interval (in seconds) for reading events from the buffer to transmit
 via jms.",
          "propertyOrder" : 7400,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "maxBatchedEvents" : {
          "title" : "Max Batched",
          "description" : "Maximum number of events per batch.",
          "propertyOrder" : 7100,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        }
      }
    },
    "commonHandler" : {
      "type" : "object",
      "title" : "General Handler Configuration",
      "propertyOrder" : 0,
      "properties" : {
        "topics" : {
          "title" : "Topics",
          "description" : "List of topics handled by an audit event handler.",
          "propertyOrder" : 6300,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
```

```
          "exampleValue" : ""
        },
        "enabled" : {
          "title" : "Enabled",
          "description" : "Enables or disables an audit event handler.",
          "propertyOrder" : 6200,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        }
      }
    },
    "jmsConfiguration" : {
      "type" : "object",
      "title" : "JMS Configuration",
      "propertyOrder" : 2,
      "properties" : {
        "deliveryMode" : {
          "title" : "Delivery Mode",
          "description" : "Specifies whether JMS messages used to transmit audit events use persistent
or non-persistent delivery.<p><p>With persistent delivery, the JMS provider ensures that messages
are not lost in transit in case of a provider failure by logging messages to storage when they are
sent.<p>Specify the delivery mode as persistent if it is unacceptable for delivery of audit events
to be lost in JMS transit. If the possible loss of audit events is acceptable, choose non-persistent
delivery, which provides better performance.",
          "propertyOrder" : 6400,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "jndiContextProperties" : {
          "title" : "JNDI Context Properties",
          "description" : "Specifies JNDI properties that OpenAM uses to connect to the JMS message
broker to which OpenAM will publish audit events.<p><p>OpenAM acts as a JMS client, using a JMS
connection factory to connect to your JMS message broker. In order for OpenAM to connect to the
broker, the JNDI context properties must conform to those needed by the broker. See the documentation
for your JMS message broker for required values.<p>The default properties are example properties for
connecting to Apache ActiveMQ.",
          "propertyOrder" : 6600,
          "required" : true,
          "patternProperties" : {
            ".*" : {
              "type" : "string"
            }
          },
          "type" : "object",
          "exampleValue" : ""
        },
        "sessionMode" : {
          "title" : "Session Mode",
          "description" : "Specifies the JMS session acknowledgement mode: <code>AUTO</code>,
<code>CLIENT</code>, or <code>DUPS_OK</code>.<p><ul><li>Auto mode guarantees once-only delivery of
JMS messages used to transmit audit events.</li><li>Duplicates OK mode ensures that messages are
delivered at least once.</li><li>Client mode does not ensure delivery.</li></ul><p>Use the default
setting unless your JMS broker implementation requires otherwise. See your broker documentation for
more information.",
          "propertyOrder" : 6500,
          "required" : true,
          "type" : "string",
```

```
          "exampleValue" : ""
        },
        "jndiConnectionFactoryName" : {
          "title" : "JMS Connection Factory Name",
          "description" : "Specifies the JNDI lookup name for the connection factory exposed by your
JMS message broker. OpenAM performs a JNDI lookup on this name to locate your broker's connection
factory.<p><p>See the documentation for your JMS message broker for the required value.<p>The default
is the connection factory name for Apache ActiveMQ.",
          "propertyOrder" : 6800,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "jndiTopicName" : {
          "title" : "JMS Topic Name",
          "description" : "JNDI lookup name for the JMS topic",
          "propertyOrder" : 6700,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "commonHandlerPlugin" : {
      "type" : "object",
      "title" : "Audit Event Handler Factory",
      "propertyOrder" : 1,
      "properties" : {
        "handlerFactory" : {
          "title" : "Factory Class Name",
          "description" : "The fully qualified class name of the factory
responsible for creating the Audit Event Handler. The class must implement
<code>org.forgerock.openam.audit.AuditEventHandlerFactory</code>.",
          "propertyOrder" : 7600,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    }
  }
}
```

delete

Usage:

```
am> delete Jms --global --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action Jms --global --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action Jms --global --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action Jms --global --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query Jms --global --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read Jms --global --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update Jms --global --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "batchEvents" : {
      "type" : "object",
      "title" : "Batch Events",
      "propertyOrder" : 3,
      "properties" : {
        "batchCapacity" : {
          "title" : "Capacity",
          "description" : "Maximum event count in the batch queue; additional events are dropped.",
          "propertyOrder" : 7000,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "pollTimeoutSec" : {
          "title" : "Writing Interval",
          "description" : "The interval (in seconds) for reading events from the buffer to transmit
 via jms.",
          "propertyOrder" : 7400,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "maxBatchedEvents" : {
          "title" : "Max Batched",
          "description" : "Maximum number of events per batch.",
          "propertyOrder" : 7100,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        }
      }
    },
    "commonHandler" : {
      "type" : "object",
      "title" : "General Handler Configuration",
      "propertyOrder" : 0,
      "properties" : {
        "topics" : {
          "title" : "Topics",
```

```
          "description" : "List of topics handled by an audit event handler.",
          "propertyOrder" : 6300,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "enabled" : {
          "title" : "Enabled",
          "description" : "Enables or disables an audit event handler.",
          "propertyOrder" : 6200,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        }
      }
    },
    "jmsConfiguration" : {
      "type" : "object",
      "title" : "JMS Configuration",
      "propertyOrder" : 2,
      "properties" : {
        "deliveryMode" : {
          "title" : "Delivery Mode",
          "description" : "Specifies whether JMS messages used to transmit audit events use persistent
or non-persistent delivery.<p><p>With persistent delivery, the JMS provider ensures that messages
are not lost in transit in case of a provider failure by logging messages to storage when they are
sent.<p>Specify the delivery mode as persistent if it is unacceptable for delivery of audit events
to be lost in JMS transit. If the possible loss of audit events is acceptable, choose non-persistent
delivery, which provides better performance.",
          "propertyOrder" : 6400,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "jndiContextProperties" : {
          "title" : "JNDI Context Properties",
          "description" : "Specifies JNDI properties that OpenAM uses to connect to the JMS message
broker to which OpenAM will publish audit events.<p><p>OpenAM acts as a JMS client, using a JMS
connection factory to connect to your JMS message broker. In order for OpenAM to connect to the
broker, the JNDI context properties must conform to those needed by the broker. See the documentation
for your JMS message broker for required values.<p>The default properties are example properties for
connecting to Apache ActiveMQ.",
          "propertyOrder" : 6600,
          "required" : true,
          "patternProperties" : {
            ".*" : {
              "type" : "string"
            }
          },
          "type" : "object",
          "exampleValue" : ""
        },
        "sessionMode" : {
          "title" : "Session Mode",
          "description" : "Specifies the JMS session acknowledgement mode: <code>AUTO</code>,
<code>CLIENT</code>, or <code>DUPS_OK</code>.<p><ul><li>Auto mode guarantees once-only delivery of
```

```
JMS messages used to transmit audit events.</li><li>Duplicates OK mode ensures that messages are
delivered at least once.</li><li>Client mode does not ensure delivery.</li></ul><p>Use the default
setting unless your JMS broker implementation requires otherwise. See your broker documentation for
more information.",
          "propertyOrder" : 6500,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "jndiConnectionFactoryName" : {
          "title" : "JMS Connection Factory Name",
          "description" : "Specifies the JNDI lookup name for the connection factory exposed by your
JMS message broker. OpenAM performs a JNDI lookup on this name to locate your broker's connection
factory.<p><p>See the documentation for your JMS message broker for the required value.<p>The default
is the connection factory name for Apache ActiveMQ.",
          "propertyOrder" : 6800,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "jndiTopicName" : {
          "title" : "JMS Topic Name",
          "description" : "JNDI lookup name for the JMS topic",
          "propertyOrder" : 6700,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "commonHandlerPlugin" : {
      "type" : "object",
      "title" : "Audit Event Handler Factory",
      "propertyOrder" : 1,
      "properties" : {
        "handlerFactory" : {
          "title" : "Factory Class Name",
          "description" : "The fully qualified class name of the factory
responsible for creating the Audit Event Handler. The class must implement
<code>org.forgerock.openam.audit.AuditEventHandlerFactory</code>.",
          "propertyOrder" : 7600,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    }
  }
}
```

Json

Realm Operations

Resource path: `/realm-config/services/audit/JSON`

Resource version: `1.0`

create

Usage:

```
am> create Json --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "jsonConfig" : {
      "type" : "object",
      "title" : "JSON Configuration",
      "propertyOrder" : 2,
      "properties" : {
        "location" : {
          "title" : "Log Directory",
          "description" : "Directory in which to store audit log JSON files.",
          "propertyOrder" : 500,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "rotationRetentionCheckInterval" : {
          "title" : "File Rotation Retention Check Interval",
          "description" : "Interval to check time-based file rotation policies, in seconds.",
          "propertyOrder" : 1800,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "elasticsearchCompatible" : {
          "title" : "ElasticSearch JSON Format Compatible",
          "description" : "JSON format should be transformed to be compatible with  ElasticSearch
 format restrictions.",
          "propertyOrder" : 1700,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        }
      }
    },
    "jsonFileRotation" : {
```

```
    "type" : "object",
    "title" : "File Rotation",
    "propertyOrder" : 3,
    "properties" : {
      "rotationFilePrefix" : {
        "title" : "File Rotation Prefix",
        "description" : "Prefix to prepend to audit files when rotating audit files.",
        "propertyOrder" : 800,
        "required" : false,
        "type" : "string",
        "exampleValue" : ""
      },
      "rotationEnabled" : {
        "title" : "Rotation Enabled",
        "description" : "Enables and disables audit file rotation.",
        "propertyOrder" : 600,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
      },
      "rotationTimes" : {
        "title" : "Rotation Times",
        "description" : "Durations after midnight to trigger file rotation, in seconds.",
        "propertyOrder" : 1100,
        "required" : true,
        "items" : {
          "type" : "string"
        },
        "type" : "array",
        "exampleValue" : ""
      },
      "rotationFileSuffix" : {
        "title" : "File Rotation Suffix",
        "description" : "Suffix to append to audit files when they are rotated. Suffix should be a
timestamp.",
        "propertyOrder" : 900,
        "required" : false,
        "type" : "string",
        "exampleValue" : ""
      },
      "rotationInterval" : {
        "title" : "Rotation Interval",
        "description" : "Interval to trigger audit file rotations, in seconds. A negative or zero
value disables this feature.",
        "propertyOrder" : 1000,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
      },
      "rotationMaxFileSize" : {
        "title" : "Maximum File Size",
        "description" : "Maximum size, in bytes, which an audit file can grow to before rotation is
triggered. A negative or zero value indicates this policy is disabled.",
        "propertyOrder" : 700,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
      }
    }
```

```
   },
   "jsonFileRetention" : {
     "type" : "object",
     "title" : "File Retention",
     "propertyOrder" : 4,
     "properties" : {
       "retentionMinFreeSpaceRequired" : {
         "title" : "Minimum Free Space Required",
         "description" : "Minimum amount of disk space required, in bytes, on the system where audit
files are stored. A negative or zero value indicates this policy is disabled.",
         "propertyOrder" : 1400,
         "required" : true,
         "type" : "string",
         "exampleValue" : ""
       },
       "retentionMaxNumberOfHistoryFiles" : {
         "title" : "Maximum Number of Historical Files",
         "description" : "Maximum number of backup audit files allowed. A value of <code>-1</code>
disables pruning of old history files.",
         "propertyOrder" : 1200,
         "required" : true,
         "type" : "string",
         "exampleValue" : ""
       },
       "retentionMaxDiskSpaceToUse" : {
         "title" : "Maximum Disk Space",
         "description" : "The maximum amount of disk space the audit files can occupy, in bytes. A
negative or zero value indicates this policy is disabled.",
         "propertyOrder" : 1300,
         "required" : true,
         "type" : "string",
         "exampleValue" : ""
       }
     }
   },
   "commonHandlerPlugin" : {
     "type" : "object",
     "title" : "Audit Event Handler Factory",
     "propertyOrder" : 1,
     "properties" : {
       "handlerFactory" : {
         "title" : "Factory Class Name",
         "description" : "The fully qualified class name of the factory
responsible for creating the Audit Event Handler. The class must implement
<code>org.forgerock.openam.audit.AuditEventHandlerFactory</code>.",
         "propertyOrder" : 1900,
         "required" : true,
         "type" : "string",
         "exampleValue" : ""
       }
     }
   },
   "jsonBuffering" : {
     "type" : "object",
     "title" : "Buffering",
     "propertyOrder" : 5,
     "properties" : {
       "bufferingWriteInterval" : {
         "title" : "Write interval",
```

```
          "description" : "Interval at which buffered events are written to a file, in milliseconds.",
          "propertyOrder" : 1600,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "bufferingMaxSize" : {
          "title" : "Batch Size",
          "description" : "Maximum number of events that can be buffered (default/minimum: 100000)",
          "propertyOrder" : 1500,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "commonHandler" : {
      "type" : "object",
      "title" : "General Handler Configuration",
      "propertyOrder" : 0,
      "properties" : {
        "topics" : {
          "title" : "Topics",
          "description" : "List of topics handled by an audit event handler.",
          "propertyOrder" : 400,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "enabled" : {
          "title" : "Enabled",
          "description" : "Enables or disables an audit event handler.",
          "propertyOrder" : 300,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        }
      }
    }
  }
}
```

delete

Usage:

```
am> delete Json --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action Json --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action Json --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action Json --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query Json --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read Json --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update Json --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "jsonConfig" : {
      "type" : "object",
      "title" : "JSON Configuration",
      "propertyOrder" : 2,
      "properties" : {
        "location" : {
          "title" : "Log Directory",
          "description" : "Directory in which to store audit log JSON files.",
          "propertyOrder" : 500,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "rotationRetentionCheckInterval" : {
          "title" : "File Rotation Retention Check Interval",
          "description" : "Interval to check time-based file rotation policies, in seconds.",
          "propertyOrder" : 1800,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "elasticsearchCompatible" : {
          "title" : "ElasticSearch JSON Format Compatible",
          "description" : "JSON format should be transformed to be compatible with  ElasticSearch
 format restrictions.",
          "propertyOrder" : 1700,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        }
      }
    },
    "jsonFileRotation" : {
      "type" : "object",
      "title" : "File Rotation",
      "propertyOrder" : 3,
      "properties" : {
        "rotationFilePrefix" : {
          "title" : "File Rotation Prefix",
```

```
          "description" : "Prefix to prepend to audit files when rotating audit files.",
          "propertyOrder" : 800,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "rotationEnabled" : {
          "title" : "Rotation Enabled",
          "description" : "Enables and disables audit file rotation.",
          "propertyOrder" : 600,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "rotationTimes" : {
          "title" : "Rotation Times",
          "description" : "Durations after midnight to trigger file rotation, in seconds.",
          "propertyOrder" : 1100,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "rotationFileSuffix" : {
          "title" : "File Rotation Suffix",
          "description" : "Suffix to append to audit files when they are rotated. Suffix should be a
timestamp.",
          "propertyOrder" : 900,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "rotationInterval" : {
          "title" : "Rotation Interval",
          "description" : "Interval to trigger audit file rotations, in seconds. A negative or zero
value disables this feature.",
          "propertyOrder" : 1000,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "rotationMaxFileSize" : {
          "title" : "Maximum File Size",
          "description" : "Maximum size, in bytes, which an audit file can grow to before rotation is
triggered. A negative or zero value indicates this policy is disabled.",
          "propertyOrder" : 700,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "jsonFileRetention" : {
      "type" : "object",
      "title" : "File Retention",
      "propertyOrder" : 4,
      "properties" : {
```

```
       "retentionMinFreeSpaceRequired" : {
         "title" : "Minimum Free Space Required",
         "description" : "Minimum amount of disk space required, in bytes, on the system where audit
files are stored. A negative or zero value indicates this policy is disabled.",
         "propertyOrder" : 1400,
         "required" : true,
         "type" : "string",
         "exampleValue" : ""
       },
       "retentionMaxNumberOfHistoryFiles" : {
         "title" : "Maximum Number of Historical Files",
         "description" : "Maximum number of backup audit files allowed. A value of <code>-1</code>
disables pruning of old history files.",
         "propertyOrder" : 1200,
         "required" : true,
         "type" : "string",
         "exampleValue" : ""
       },
       "retentionMaxDiskSpaceToUse" : {
         "title" : "Maximum Disk Space",
         "description" : "The maximum amount of disk space the audit files can occupy, in bytes. A
negative or zero value indicates this policy is disabled.",
         "propertyOrder" : 1300,
         "required" : true,
         "type" : "string",
         "exampleValue" : ""
       }
     }
   },
   "commonHandlerPlugin" : {
     "type" : "object",
     "title" : "Audit Event Handler Factory",
     "propertyOrder" : 1,
     "properties" : {
       "handlerFactory" : {
         "title" : "Factory Class Name",
         "description" : "The fully qualified class name of the factory
responsible for creating the Audit Event Handler. The class must implement
<code>org.forgerock.openam.audit.AuditEventHandlerFactory</code>.",
         "propertyOrder" : 1900,
         "required" : true,
         "type" : "string",
         "exampleValue" : ""
       }
     }
   },
   "jsonBuffering" : {
     "type" : "object",
     "title" : "Buffering",
     "propertyOrder" : 5,
     "properties" : {
       "bufferingWriteInterval" : {
         "title" : "Write interval",
         "description" : "Interval at which buffered events are written to a file, in milliseconds.",
         "propertyOrder" : 1600,
         "required" : true,
         "type" : "string",
         "exampleValue" : ""
       },
```

```
        "bufferingMaxSize" : {
          "title" : "Batch Size",
          "description" : "Maximum number of events that can be buffered (default/minimum: 100000)",
          "propertyOrder" : 1500,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "commonHandler" : {
      "type" : "object",
      "title" : "General Handler Configuration",
      "propertyOrder" : 0,
      "properties" : {
        "topics" : {
          "title" : "Topics",
          "description" : "List of topics handled by an audit event handler.",
          "propertyOrder" : 400,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "enabled" : {
          "title" : "Enabled",
          "description" : "Enables or disables an audit event handler.",
          "propertyOrder" : 300,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        }
      }
    }
  }
}
```

Global Operations

Resource path: `/global-config/services/audit/JSON`

Resource version: `1.0`

create

Usage:

```
am> create Json --global --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "commonHandlerPlugin" : {
      "type" : "object",
      "title" : "Audit Event Handler Factory",
      "propertyOrder" : 1,
      "properties" : {
        "handlerFactory" : {
          "title" : "Factory Class Name",
          "description" : "The fully qualified class name of the factory
 responsible for creating the Audit Event Handler. The class must implement
 <code>org.forgerock.openam.audit.AuditEventHandlerFactory</code>.",
          "propertyOrder" : 1900,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "jsonBuffering" : {
      "type" : "object",
      "title" : "Buffering",
      "propertyOrder" : 5,
      "properties" : {
        "bufferingMaxSize" : {
          "title" : "Batch Size",
          "description" : "Maximum number of events that can be buffered (default/minimum: 100000)",
          "propertyOrder" : 1500,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "bufferingWriteInterval" : {
          "title" : "Write interval",
          "description" : "Interval at which buffered events are written to a file, in milliseconds.",
          "propertyOrder" : 1600,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "jsonConfig" : {
      "type" : "object",
      "title" : "JSON Configuration",
      "propertyOrder" : 2,
      "properties" : {
        "rotationRetentionCheckInterval" : {
          "title" : "File Rotation Retention Check Interval",
          "description" : "Interval to check time-based file rotation policies, in seconds.",
```

```
          "propertyOrder" : 1800,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "elasticsearchCompatible" : {
          "title" : "ElasticSearch JSON Format Compatible",
          "description" : "JSON format should be transformed to be compatible with  ElasticSearch
format restrictions.",
          "propertyOrder" : 1700,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "location" : {
          "title" : "Log Directory",
          "description" : "Directory in which to store audit log JSON files.",
          "propertyOrder" : 500,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "jsonFileRotation" : {
      "type" : "object",
      "title" : "File Rotation",
      "propertyOrder" : 3,
      "properties" : {
        "rotationMaxFileSize" : {
          "title" : "Maximum File Size",
          "description" : "Maximum size, in bytes, which an audit file can grow to before rotation is
triggered. A negative or zero value indicates this policy is disabled.",
          "propertyOrder" : 700,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "rotationTimes" : {
          "title" : "Rotation Times",
          "description" : "Durations after midnight to trigger file rotation, in seconds.",
          "propertyOrder" : 1100,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "rotationFileSuffix" : {
          "title" : "File Rotation Suffix",
          "description" : "Suffix to append to audit files when they are rotated. Suffix should be a
timestamp.",
          "propertyOrder" : 900,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "rotationInterval" : {
```

```
          "title" : "Rotation Interval",
          "description" : "Interval to trigger audit file rotations, in seconds. A negative or zero
value disables this feature.",
          "propertyOrder" : 1000,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "rotationEnabled" : {
          "title" : "Rotation Enabled",
          "description" : "Enables and disables audit file rotation.",
          "propertyOrder" : 600,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "rotationFilePrefix" : {
          "title" : "File Rotation Prefix",
          "description" : "Prefix to prepend to audit files when rotating audit files.",
          "propertyOrder" : 800,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "jsonFileRetention" : {
      "type" : "object",
      "title" : "File Retention",
      "propertyOrder" : 4,
      "properties" : {
        "retentionMinFreeSpaceRequired" : {
          "title" : "Minimum Free Space Required",
          "description" : "Minimum amount of disk space required, in bytes, on the system where audit
files are stored. A negative or zero value indicates this policy is disabled.",
          "propertyOrder" : 1400,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "retentionMaxNumberOfHistoryFiles" : {
          "title" : "Maximum Number of Historical Files",
          "description" : "Maximum number of backup audit files allowed. A value of <code>-1</code>
disables pruning of old history files.",
          "propertyOrder" : 1200,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "retentionMaxDiskSpaceToUse" : {
          "title" : "Maximum Disk Space",
          "description" : "The maximum amount of disk space the audit files can occupy, in bytes. A
negative or zero value indicates this policy is disabled.",
          "propertyOrder" : 1300,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      }
```

```
    },
    "commonHandler" : {
      "type" : "object",
      "title" : "General Handler Configuration",
      "propertyOrder" : 0,
      "properties" : {
        "topics" : {
          "title" : "Topics",
          "description" : "List of topics handled by an audit event handler.",
          "propertyOrder" : 400,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "enabled" : {
          "title" : "Enabled",
          "description" : "Enables or disables an audit event handler.",
          "propertyOrder" : 300,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        }
      }
    }
  }
}
```

delete

Usage:

```
am> delete Json --global --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action Json --global --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action Json --global --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action Json --global --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query Json --global --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read Json --global --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update Json --global --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "commonHandlerPlugin" : {
      "type" : "object",
      "title" : "Audit Event Handler Factory",
      "propertyOrder" : 1,
      "properties" : {
        "handlerFactory" : {
          "title" : "Factory Class Name",
          "description" : "The fully qualified class name of the factory
 responsible for creating the Audit Event Handler. The class must implement
 <code>org.forgerock.openam.audit.AuditEventHandlerFactory</code>.",
          "propertyOrder" : 1900,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "jsonBuffering" : {
      "type" : "object",
      "title" : "Buffering",
      "propertyOrder" : 5,
      "properties" : {
        "bufferingMaxSize" : {
          "title" : "Batch Size",
          "description" : "Maximum number of events that can be buffered (default/minimum: 100000)",
          "propertyOrder" : 1500,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "bufferingWriteInterval" : {
          "title" : "Write interval",
          "description" : "Interval at which buffered events are written to a file, in milliseconds.",
          "propertyOrder" : 1600,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "jsonConfig" : {
      "type" : "object",
      "title" : "JSON Configuration",
      "propertyOrder" : 2,
      "properties" : {
        "rotationRetentionCheckInterval" : {
          "title" : "File Rotation Retention Check Interval",
          "description" : "Interval to check time-based file rotation policies, in seconds.",
          "propertyOrder" : 1800,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
```

```
       },
       "elasticsearchCompatible" : {
         "title" : "ElasticSearch JSON Format Compatible",
         "description" : "JSON format should be transformed to be compatible with  ElasticSearch
format restrictions.",
         "propertyOrder" : 1700,
         "required" : true,
         "type" : "boolean",
         "exampleValue" : ""
       },
       "location" : {
         "title" : "Log Directory",
         "description" : "Directory in which to store audit log JSON files.",
         "propertyOrder" : 500,
         "required" : true,
         "type" : "string",
         "exampleValue" : ""
       }
     }
   },
   "jsonFileRotation" : {
     "type" : "object",
     "title" : "File Rotation",
     "propertyOrder" : 3,
     "properties" : {
       "rotationMaxFileSize" : {
         "title" : "Maximum File Size",
         "description" : "Maximum size, in bytes, which an audit file can grow to before rotation is
triggered. A negative or zero value indicates this policy is disabled.",
         "propertyOrder" : 700,
         "required" : true,
         "type" : "string",
         "exampleValue" : ""
       },
       "rotationTimes" : {
         "title" : "Rotation Times",
         "description" : "Durations after midnight to trigger file rotation, in seconds.",
         "propertyOrder" : 1100,
         "required" : true,
         "items" : {
           "type" : "string"
         },
         "type" : "array",
         "exampleValue" : ""
       },
       "rotationFileSuffix" : {
         "title" : "File Rotation Suffix",
         "description" : "Suffix to append to audit files when they are rotated. Suffix should be a
timestamp.",
         "propertyOrder" : 900,
         "required" : false,
         "type" : "string",
         "exampleValue" : ""
       },
       "rotationInterval" : {
         "title" : "Rotation Interval",
         "description" : "Interval to trigger audit file rotations, in seconds. A negative or zero
value disables this feature.",
         "propertyOrder" : 1000,
```

```
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "rotationEnabled" : {
          "title" : "Rotation Enabled",
          "description" : "Enables and disables audit file rotation.",
          "propertyOrder" : 600,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "rotationFilePrefix" : {
          "title" : "File Rotation Prefix",
          "description" : "Prefix to prepend to audit files when rotating audit files.",
          "propertyOrder" : 800,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "jsonFileRetention" : {
      "type" : "object",
      "title" : "File Retention",
      "propertyOrder" : 4,
      "properties" : {
        "retentionMinFreeSpaceRequired" : {
          "title" : "Minimum Free Space Required",
          "description" : "Minimum amount of disk space required, in bytes, on the system where audit
files are stored. A negative or zero value indicates this policy is disabled.",
          "propertyOrder" : 1400,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "retentionMaxNumberOfHistoryFiles" : {
          "title" : "Maximum Number of Historical Files",
          "description" : "Maximum number of backup audit files allowed. A value of <code>-1</code>
disables pruning of old history files.",
          "propertyOrder" : 1200,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "retentionMaxDiskSpaceToUse" : {
          "title" : "Maximum Disk Space",
          "description" : "The maximum amount of disk space the audit files can occupy, in bytes. A
negative or zero value indicates this policy is disabled.",
          "propertyOrder" : 1300,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "commonHandler" : {
      "type" : "object",
      "title" : "General Handler Configuration",
```

```
      "propertyOrder" : 0,
      "properties" : {
        "topics" : {
          "title" : "Topics",
          "description" : "List of topics handled by an audit event handler.",
          "propertyOrder" : 400,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "enabled" : {
          "title" : "Enabled",
          "description" : "Enables or disables an audit event handler.",
          "propertyOrder" : 300,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        }
      }
    }
  }
}
```

JwtProofOfPossessionModule

Realm Operations

Resource path: `/realm-config/authentication/modules/authJwtPoP`

Resource version: `1.0`

create

Usage:

```
am> create JwtProofOfPossessionModule --realm Realm --id id --body body
```

Parameters:

`--id`

The unique identifier for the resource.

`--body`

The resource in JSON format, described by the following JSON schema:

```
{
```

```
  "type" : "object",
  "properties" : {
    "challengeSigningKey" : {
      "title" : "Challenge Signing Key",
      "description" : "Name of the key (in the AM keystore) to use to sign challenges.",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "subjectJwkSetAttr" : {
      "title" : "Subject JWK Set Attribute",
      "description" : "Subject profile attribute that contains a JWK Set of confirmation and
 encryption keys.",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "responseEncryptionCipher" : {
      "title" : "Response Encryption Cipher",
      "description" : "The authenticated encryption (AEAD) scheme to use for the response.",
      "propertyOrder" : 350,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "authenticationLevel" : {
      "title" : "Authentication Level",
      "description" : "The authentication level associated with this module.",
      "propertyOrder" : 10000,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "responseEncryptionMethod" : {
      "title" : "Response Encryption Scheme",
      "description" : "Key exchange method to use for responses: ephemeral elliptic curve Diffie-
Hellman (ECDHE)key agreement or using a pre-shared key (PSK) from the subject's JWK Set.",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "enableTlsSessionBinding" : {
      "title" : "Use TLS Session Binding",
      "description" : "If enabled the response must arrive in the same TLS (HTTPS) session as the
 challenge was issued.",
      "propertyOrder" : 400,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    }
  }
}
```

delete

Usage:

```
am> delete JwtProofOfPossessionModule --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action JwtProofOfPossessionModule --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action JwtProofOfPossessionModule --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action JwtProofOfPossessionModule --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query JwtProofOfPossessionModule --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read JwtProofOfPossessionModule --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update JwtProofOfPossessionModule --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "challengeSigningKey" : {
      "title" : "Challenge Signing Key",
      "description" : "Name of the key (in the AM keystore) to use to sign challenges.",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "subjectJwkSetAttr" : {
      "title" : "Subject JWK Set Attribute",
      "description" : "Subject profile attribute that contains a JWK Set of confirmation and
 encryption keys.",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "responseEncryptionCipher" : {
      "title" : "Response Encryption Cipher",
      "description" : "The authenticated encryption (AEAD) scheme to use for the response.",
      "propertyOrder" : 350,
```

```
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "authenticationLevel" : {
      "title" : "Authentication Level",
      "description" : "The authentication level associated with this module.",
      "propertyOrder" : 10000,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "responseEncryptionMethod" : {
      "title" : "Response Encryption Scheme",
      "description" : "Key exchange method to use for responses: ephemeral elliptic curve Diffie-
Hellman (ECDHE)key agreement or using a pre-shared key (PSK) from the subject's JWK Set.",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "enableTlsSessionBinding" : {
      "title" : "Use TLS Session Binding",
      "description" : "If enabled the response must arrive in the same TLS (HTTPS) session as the
 challenge was issued.",
      "propertyOrder" : 400,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    }
  }
}
```

Global Operations

Resource path: `/global-config/authentication/modules/authJwtPoP`

Resource version: `1.0`

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action JwtProofOfPossessionModule --global --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action JwtProofOfPossessionModule --global --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action JwtProofOfPossessionModule --global --actionName nextdescendents
```

read

Usage:

```
am> read JwtProofOfPossessionModule --global
```

update

Usage:

```
am> update JwtProofOfPossessionModule --global --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "defaults" : {
      "properties" : {
        "subjectJwkSetAttr" : {
          "title" : "Subject JWK Set Attribute",
          "description" : "Subject profile attribute that contains a JWK Set of confirmation and
 encryption keys.",
          "propertyOrder" : 100,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "authenticationLevel" : {
          "title" : "Authentication Level",
          "description" : "The authentication level associated with this module.",
          "propertyOrder" : 10000,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "responseEncryptionCipher" : {
          "title" : "Response Encryption Cipher",
```

```
          "description" : "The authenticated encryption (AEAD) scheme to use for the response.",
          "propertyOrder" : 350,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "responseEncryptionMethod" : {
          "title" : "Response Encryption Scheme",
          "description" : "Key exchange method to use for responses: ephemeral elliptic curve Diffie-
Hellman (ECDHE)key agreement or using a pre-shared key (PSK) from the subject's JWK Set.",
          "propertyOrder" : 300,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "challengeSigningKey" : {
          "title" : "Challenge Signing Key",
          "description" : "Name of the key (in the AM keystore) to use to sign challenges.",
          "propertyOrder" : 200,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "enableTlsSessionBinding" : {
          "title" : "Use TLS Session Binding",
          "description" : "If enabled the response must arrive in the same TLS (HTTPS) session as the
 challenge was issued.",
          "propertyOrder" : 400,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        }
      },
      "type" : "object",
      "title" : "Realm Defaults"
    }
  }
}
```

KBADecision

Realm Operations

Resource path: `/realm-config/authentication/authenticationtrees/nodes/KbaDecisionNode`

Resource version: `1.0`

create

Usage:

```
am> create KBADecision --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "identityAttribute" : {
      "title" : "Identity Attribute",
      "description" : "The attribute of the IDM object to use retrieve the object.",
      "propertyOrder" : 100,
      "type" : "string",
      "exampleValue" : ""
    }
  },
  "required" : [ "identityAttribute" ]
}
```

delete

Usage:

```
am> delete KBADecision --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action KBADecision --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action KBADecision --realm Realm --actionName getCreatableTypes
```

listOutcomes

List the available outcomes for the node type.

Usage:

```
am> action KBADecision --realm Realm --body body --actionName listOutcomes
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "title" : "Some configuration of the node. This does not need to be complete against the
 configuration schema."
}
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action KBADecision --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query KBADecision --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read KBADecision --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update KBADecision --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "identityAttribute" : {
      "title" : "Identity Attribute",
      "description" : "The attribute of the IDM object to use retrieve the object.",
      "propertyOrder" : 100,
      "type" : "string",
      "exampleValue" : ""
    }
  },
  "required" : [ "identityAttribute" ]
}
```

KBADefinition

Realm Operations

Resource path: `/realm-config/authentication/authenticationtrees/nodes/KbaCreateNode`

Resource version: `1.0`

create

Usage:

```
am> create KBADefinition --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "message" : {
      "title" : "Purpose Message",
      "description" : "Localised message describing the purpose of the data requested from the user.",
      "propertyOrder" : 100,
      "patternProperties" : {
        ".*" : {
          "type" : "string"
        }
      },
      "type" : "object",
      "exampleValue" : ""
    }
  },
  "required" : [ "message" ]
}
```

delete

Usage:

```
am> delete KBADefinition --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action KBADefinition --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action KBADefinition --realm Realm --actionName getCreatableTypes
```

listOutcomes

List the available outcomes for the node type.

Usage:

```
am> action KBADefinition --realm Realm --body body --actionName listOutcomes
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "title" : "Some configuration of the node. This does not need to be complete against the
 configuration schema."
}
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action KBADefinition --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query KBADefinition --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read KBADefinition --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update KBADefinition --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "message" : {
      "title" : "Purpose Message",
      "description" : "Localised message describing the purpose of the data requested from the user.",
      "propertyOrder" : 100,
      "patternProperties" : {
        ".*" : {
          "type" : "string"
        }
      },
      "type" : "object",
      "exampleValue" : ""
    }
  },
  "required" : [ "message" ]
}
```

KBAVerification

Realm Operations

Resource path: `/realm-config/authentication/authenticationtrees/nodes/KbaVerifyNode`

Resource version: `1.0`

create

Usage:

```
am> create KBAVerification --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "kbaInfoAttribute" : {
      "title" : "KBA Attribute",
      "description" : "The attribute in the user object in IDM where KBA questions and answers are
 stored.",
      "propertyOrder" : 100,
      "type" : "string",
      "exampleValue" : ""
    },
    "identityAttribute" : {
      "title" : "Identity Attribute",
      "description" : "The IDM attribute used to identify the object in a search, e.g. userName.",
      "propertyOrder" : 200,
      "type" : "string",
      "exampleValue" : ""
    }
  },
  "required" : [ "kbaInfoAttribute", "identityAttribute" ]
}
```

delete

Usage:

```
am> delete KBAVerification --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action KBAVerification --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action KBAVerification --realm Realm --actionName getCreatableTypes
```

listOutcomes

List the available outcomes for the node type.

Usage:

```
am> action KBAVerification --realm Realm --body body --actionName listOutcomes
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "title" : "Some configuration of the node. This does not need to be complete against the
 configuration schema."
}
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action KBAVerification --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query KBAVerification --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read KBAVerification --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update KBAVerification --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "kbaInfoAttribute" : {
      "title" : "KBA Attribute",
      "description" : "The attribute in the user object in IDM where KBA questions and answers are
 stored.",
      "propertyOrder" : 100,
      "type" : "string",
      "exampleValue" : ""
    },
    "identityAttribute" : {
      "title" : "Identity Attribute",
      "description" : "The IDM attribute used to identify the object in a search, e.g. userName.",
      "propertyOrder" : 200,
      "type" : "string",
      "exampleValue" : ""
    }
  },
  "required" : [ "kbaInfoAttribute", "identityAttribute" ]
}
```

KbaQuestions

Realm Operations

KBA resource is responsible for delivering up configured security questions.

Resource path: `/selfservice/kba`

Resource version: `1.0`

read

Read the configured security questions.

Usage:

```
am> read KbaQuestions --realm Realm
```

KerberosNode

Realm Operations

Resource path: `/realm-config/authentication/authenticationtrees/nodes/product-KerberosNode`

Resource version: `1.0`

create

Usage:

```
am> create KerberosNode --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "returnPrincipalWithDomainName" : {
      "title" : "Return Principal with Domain Name",
      "description" : "Returns the fully qualified name of the authenticated user rather than just the
 username.",
      "propertyOrder" : 600,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "kerberosServiceIsInitiator" : {
      "title" : "Is Initiator",
      "description" : "True, if initiator. False, if acceptor only. Default is True.",
      "propertyOrder" : 800,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "kerberosRealm" : {
      "title" : "Kerberos Realm",
      "description" : "The name of the Kerberos (Active Directory) realm used for authentication.",
      "propertyOrder" : 300,
      "type" : "string",
      "exampleValue" : ""
    },
    "kerberosServerName" : {
      "title" : "Kerberos Server Name",
      "description" : "The hostname/IP address of the Kerberos (Active Directory) server.",
      "propertyOrder" : 400,
      "type" : "string",
      "exampleValue" : ""
    },
    "lookupUserInRealm" : {
      "title" : "Lookup User In Realm",
      "description" : "Validate that the user has a matched user profile configured in the data
 store.",
      "propertyOrder" : 700,
```

```
      "type" : "boolean",
      "exampleValue" : ""
    },
    "principalName" : {
      "title" : "Service Principal",
      "description" : "The name of the Kerberos principal used during authentication. The format of
 the field is as follows:<br/><br/><code>HTTP/openam.forgerock.com@AD_DOMAIN.COM</code>",
      "propertyOrder" : 100,
      "type" : "string",
      "exampleValue" : ""
    },
    "keytabFileName" : {
      "title" : "Key Tab File Path",
      "description" : "The absolute pathname of the AD keytab file.",
      "propertyOrder" : 200,
      "type" : "string",
      "exampleValue" : ""
    },
    "trustedKerberosRealms" : {
      "title" : "Trusted Kerberos realms",
      "description" : "List of Trusted Kerberos Realms for User Kerberos tickets.",
      "propertyOrder" : 500,
      "items" : {
        "type" : "string"
      },
      "minItems" : 1,
      "type" : "array",
      "exampleValue" : ""
    }
  },
  "required" : [ "kerberosRealm", "principalName", "returnPrincipalWithDomainName",
 "trustedKerberosRealms", "kerberosServiceIsInitiator", "keytabFileName", "kerberosServerName",
 "lookupUserInRealm" ]
}
```

delete

Usage:

```
am> delete KerberosNode --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action KerberosNode --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action KerberosNode --realm Realm --actionName getCreatableTypes
```

listOutcomes

List the available outcomes for the node type.

Usage:

```
am> action KerberosNode --realm Realm --body body --actionName listOutcomes
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "title" : "Some configuration of the node. This does not need to be complete against the
 configuration schema."
}
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action KerberosNode --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query KerberosNode --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read KerberosNode --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update KerberosNode --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "returnPrincipalWithDomainName" : {
      "title" : "Return Principal with Domain Name",
      "description" : "Returns the fully qualified name of the authenticated user rather than just the
 username.",
      "propertyOrder" : 600,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "kerberosServiceIsInitiator" : {
      "title" : "Is Initiator",
      "description" : "True, if initiator. False, if acceptor only. Default is True.",
      "propertyOrder" : 800,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "kerberosRealm" : {
      "title" : "Kerberos Realm",
      "description" : "The name of the Kerberos (Active Directory) realm used for authentication.",
      "propertyOrder" : 300,
      "type" : "string",
      "exampleValue" : ""
```

```
    },
    "kerberosServerName" : {
      "title" : "Kerberos Server Name",
      "description" : "The hostname/IP address of the Kerberos (Active Directory) server.",
      "propertyOrder" : 400,
      "type" : "string",
      "exampleValue" : ""
    },
    "lookupUserInRealm" : {
      "title" : "Lookup User In Realm",
      "description" : "Validate that the user has a matched user profile configured in the data
 store.",
      "propertyOrder" : 700,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "principalName" : {
      "title" : "Service Principal",
      "description" : "The name of the Kerberos principal used during authentication. The format of
 the field is as follows:<br/><br/><code>HTTP/openam.forgerock.com@AD_DOMAIN.COM</code>",
      "propertyOrder" : 100,
      "type" : "string",
      "exampleValue" : ""
    },
    "keytabFileName" : {
      "title" : "Key Tab File Path",
      "description" : "The absolute pathname of the AD keytab file.",
      "propertyOrder" : 200,
      "type" : "string",
      "exampleValue" : ""
    },
    "trustedKerberosRealms" : {
      "title" : "Trusted Kerberos realms",
      "description" : "List of Trusted Kerberos Realms for User Kerberos tickets.",
      "propertyOrder" : 500,
      "items" : {
        "type" : "string"
      },
      "minItems" : 1,
      "type" : "array",
      "exampleValue" : ""
    }
  },
  "required" : [ "kerberosRealm", "principalName", "returnPrincipalWithDomainName",
 "trustedKerberosRealms", "kerberosServiceIsInitiator", "keytabFileName", "kerberosServerName",
 "lookupUserInRealm" ]
}
```


KeyStoreMappings

Realm Operations

Resource path: `/realm-config/secrets/stores/KeyStoreSecretStore/{KeyStoreSecretStore}/mappings`

Resource version: `1.0`

create

Usage:

```
am> create KeyStoreMappings --realm Realm --KeyStoreSecretStore KeyStoreSecretStore --id id --body body
```

Parameters:

--KeyStoreSecretStore

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "secretId" : {
      "title" : "Secret ID",
      "description" : "The secret ID that is to be associated with an alias.",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "aliases" : {
      "title" : "Aliases",
      "description" : "The list of keystore aliases that can resolve the secret. The first element of
 the alias list determines which alias is the \"active\" one. Active secrets are used for signature
 generation and encryption, while the non-active secrets are mainly used for signature verification
 and decryption.",
      "propertyOrder" : 200,
      "required" : true,
      "items" : {
        "type" : "string",
        "minLength" : 1
      },
      "minItems" : 1,
      "uniqueItems" : true,
      "type" : "array",
      "exampleValue" : ""
    }
  }
}
```

delete

Usage:

```
am> delete KeyStoreMappings --realm Realm --KeyStoreSecretStore KeyStoreSecretStore --id id
```

Parameters:

--KeyStoreSecretStore

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action KeyStoreMappings --realm Realm --KeyStoreSecretStore KeyStoreSecretStore --actionName
 getAllTypes
```

Parameters:

--KeyStoreSecretStore

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action KeyStoreMappings --realm Realm --KeyStoreSecretStore KeyStoreSecretStore --actionName
 getCreatableTypes
```

Parameters:

--KeyStoreSecretStore

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action KeyStoreMappings --realm Realm --KeyStoreSecretStore KeyStoreSecretStore --actionName
 nextdescendents
```

Parameters:

--KeyStoreSecretStore

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query KeyStoreMappings --realm Realm --KeyStoreSecretStore KeyStoreSecretStore --filter filter
```

Parameters:

--KeyStoreSecretStore

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read KeyStoreMappings --realm Realm --KeyStoreSecretStore KeyStoreSecretStore --id id
```

Parameters:

--KeyStoreSecretStore

--id

The unique identifier for the resource.

update

Usage:

```
am> update KeyStoreMappings --realm Realm --KeyStoreSecretStore KeyStoreSecretStore --id id --body body
```

Parameters:

--KeyStoreSecretStore

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "secretId" : {
      "title" : "Secret ID",
      "description" : "The secret ID that is to be associated with an alias.",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "aliases" : {
      "title" : "Aliases",
      "description" : "The list of keystore aliases that can resolve the secret. The first element of
 the alias list determines which alias is the \"active\" one. Active secrets are used for signature
 generation and encryption, while the non-active secrets are mainly used for signature verification
 and decryption.",
      "propertyOrder" : 200,
      "required" : true,
      "items" : {
        "type" : "string",
        "minLength" : 1
      },
      "minItems" : 1,
      "uniqueItems" : true,
      "type" : "array",
      "exampleValue" : ""
    }
  }
}
```

Global Operations

Resource path: `/global-config/secrets/stores/KeyStoreSecretStore/{KeyStoreSecretStore}/mappings`

Resource version: `1.0`

create

Usage:

```
am> create KeyStoreMappings --global --KeyStoreSecretStore KeyStoreSecretStore --id id --body body
```

Parameters:

--KeyStoreSecretStore

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "aliases" : {
      "title" : "Aliases",
      "description" : "The list of keystore aliases that can resolve the secret. The first element of
 the alias list determines which alias is the \"active\" one. Active secrets are used for signature
 generation and encryption, while the non-active secrets are mainly used for signature verification
 and decryption.",
      "propertyOrder" : 200,
      "required" : true,
      "items" : {
        "type" : "string",
        "minLength" : 1
      },
      "minItems" : 1,
      "uniqueItems" : true,
      "type" : "array",
      "exampleValue" : ""
    },
    "secretId" : {
      "title" : "Secret ID",
      "description" : "The secret ID that is to be associated with an alias.",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
```

delete

Usage:

```
am> delete KeyStoreMappings --global --KeyStoreSecretStore KeyStoreSecretStore --id id
```

Parameters:

--KeyStoreSecretStore

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action KeyStoreMappings --global --KeyStoreSecretStore KeyStoreSecretStore --actionName getAllTypes
```

Parameters:

--KeyStoreSecretStore

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action KeyStoreMappings --global --KeyStoreSecretStore KeyStoreSecretStore --actionName
 getCreatableTypes
```

Parameters:

--KeyStoreSecretStore

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action KeyStoreMappings --global --KeyStoreSecretStore KeyStoreSecretStore --actionName
 nextdescendents
```

Parameters:

--KeyStoreSecretStore

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query KeyStoreMappings --global --KeyStoreSecretStore KeyStoreSecretStore --filter filter
```

Parameters:

--KeyStoreSecretStore

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read KeyStoreMappings --global --KeyStoreSecretStore KeyStoreSecretStore --id id
```

Parameters:

--KeyStoreSecretStore

--id

The unique identifier for the resource.

update

Usage:

```
am> update KeyStoreMappings --global --KeyStoreSecretStore KeyStoreSecretStore --id id --body body
```

Parameters:

--KeyStoreSecretStore

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "aliases" : {
      "title" : "Aliases",
      "description" : "The list of keystore aliases that can resolve the secret. The first element of
 the alias list determines which alias is the \"active\" one. Active secrets are used for signature
 generation and encryption, while the non-active secrets are mainly used for signature verification
 and decryption.",
      "propertyOrder" : 200,
      "required" : true,
      "items" : {
        "type" : "string",
        "minLength" : 1
      },
      "minItems" : 1,
      "uniqueItems" : true,
      "type" : "array",
      "exampleValue" : ""
    },
    "secretId" : {
      "title" : "Secret ID",
      "description" : "The secret ID that is to be associated with an alias.",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
```


KeyStoreSecretStore

Realm Operations

Resource path: `/realm-config/secrets/stores/KeyStoreSecretStore`

Resource version: `1.0`

create

Usage:

```
am> create KeyStoreSecretStore --realm Realm --id id --body body
```

Parameters:

`--id`

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "leaseExpiryDuration" : {
      "title" : "Key lease expiry",
      "description" : "The amount of minutes a key can be cached from the keystore before it needs to
 be reloaded.",
      "propertyOrder" : 600,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "file" : {
      "title" : "File",
      "description" : "The keystore file to use",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "storetype" : {
      "title" : "Keystore type",
      "description" : "The type of the keystore (JKS, JCEKS, PKCS11, PKCS12, others). This must be a
 keystore type known or configured on the JRE.",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "storePassword" : {
      "title" : "Store password secret ID",
      "description" : "The secret ID from which the store password can be obtained, or none if
 the password is blank. This secret ID will be resolved using one of the other secret stores
 configured.<br> It must not start or end with the <code>.</code> character <br>The <code>.</code>
 character must not be followed by another <code>.</code> character.<br>Must contain <code>a-z</code>,
 <code>A-Z</code>, <code>0-9</code> and <code>.</code> characters only.",
      "propertyOrder" : 400,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
    },
    "keyEntryPassword" : {
      "title" : "Entry password secret ID",
      "description" : "The secret value from which the entry password can be obtained, or none
 if the password is blank. This secret ID will be resolved using one of the other secret stores
 configured.<br> It must not start or end with the <code>.</code> character. <br>The <code>.</code>
 character must not be followed by another <code>.</code> character.<br>Must contain <code>a-z</code>,
 <code>A-Z</code>, <code>0-9</code> and <code>.</code> characters only.",
      "propertyOrder" : 500,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
    },
    "providerName" : {
      "title" : "Provider name",
```

```
      "description" : "The classname of a provider to use to load the keystore. If blank, the JRE
 default will be used.",
      "propertyOrder" : 300,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
```

delete

Usage:

```
am> delete KeyStoreSecretStore --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action KeyStoreSecretStore --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action KeyStoreSecretStore --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action KeyStoreSecretStore --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query KeyStoreSecretStore --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read KeyStoreSecretStore --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update KeyStoreSecretStore --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "leaseExpiryDuration" : {
      "title" : "Key lease expiry",
      "description" : "The amount of minutes a key can be cached from the keystore before it needs to
 be reloaded.",
      "propertyOrder" : 600,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
```

```
    "file" : {
      "title" : "File",
      "description" : "The keystore file to use",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "storetype" : {
      "title" : "Keystore type",
      "description" : "The type of the keystore (JKS, JCEKS, PKCS11, PKCS12, others). This must be a
 keystore type known or configured on the JRE.",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "storePassword" : {
      "title" : "Store password secret ID",
      "description" : "The secret ID from which the store password can be obtained, or none if
 the password is blank. This secret ID will be resolved using one of the other secret stores
 configured.<br> It must not start or end with the <code>.</code> character <br>The <code>.</code>
 character must not be followed by another <code>.</code> character.<br>Must contain <code>a-z</code>,
 <code>A-Z</code>, <code>0-9</code> and <code>.</code> characters only.",
      "propertyOrder" : 400,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
    },
    "keyEntryPassword" : {
      "title" : "Entry password secret ID",
      "description" : "The secret value from which the entry password can be obtained, or none
 if the password is blank. This secret ID will be resolved using one of the other secret stores
 configured.<br> It must not start or end with the <code>.</code> character. <br>The <code>.</code>
 character must not be followed by another <code>.</code> character.<br>Must contain <code>a-z</code>,
 <code>A-Z</code>, <code>0-9</code> and <code>.</code> characters only.",
      "propertyOrder" : 500,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
    },
    "providerName" : {
      "title" : "Provider name",
      "description" : "The classname of a provider to use to load the keystore. If blank, the JRE
 default will be used.",
      "propertyOrder" : 300,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
```

Global Operations

Resource path: `/global-config/secrets/stores/KeyStoreSecretStore`

Resource version: `1.0`

create

Usage:

```
am> create KeyStoreSecretStore --global --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "file" : {
      "title" : "File",
      "description" : "The keystore file to use",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "storePassword" : {
      "title" : "Store password secret ID",
      "description" : "The secret ID from which the store password can be obtained, or none if
 the password is blank. This secret ID will be resolved using one of the other secret stores
 configured.<br> It must not start or end with the <code>.</code> character <br>The <code>.</code>
 character must not be followed by another <code>.</code> character.<br>Must contain <code>a-z</code>,
 <code>A-Z</code>, <code>0-9</code> and <code>.</code> characters only.",
      "propertyOrder" : 400,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
    },
    "storetype" : {
      "title" : "Keystore type",
      "description" : "The type of the keystore (JKS, JCEKS, PKCS11, PKCS12, others). This must be a
 keystore type known or configured on the JRE.",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "leaseExpiryDuration" : {
      "title" : "Key lease expiry",
      "description" : "The amount of minutes a key can be cached from the keystore before it needs to
 be reloaded.",
      "propertyOrder" : 600,
```

```
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "providerName" : {
      "title" : "Provider name",
      "description" : "The classname of a provider to use to load the keystore. If blank, the JRE
 default will be used.",
      "propertyOrder" : 300,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
    },
    "keyEntryPassword" : {
      "title" : "Entry password secret ID",
      "description" : "The secret value from which the entry password can be obtained, or none
 if the password is blank. This secret ID will be resolved using one of the other secret stores
 configured.<br> It must not start or end with the <code>.</code> character. <br>The <code>.</code>
 character must not be followed by another <code>.</code> character.<br>Must contain <code>a-z</code>,
 <code>A-Z</code>, <code>0-9</code> and <code>.</code> characters only.",
      "propertyOrder" : 500,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
```

delete

Usage:

```
am> delete KeyStoreSecretStore --global --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action KeyStoreSecretStore --global --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action KeyStoreSecretStore --global --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action KeyStoreSecretStore --global --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query KeyStoreSecretStore --global --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read KeyStoreSecretStore --global --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update KeyStoreSecretStore --global --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "file" : {
      "title" : "File",
      "description" : "The keystore file to use",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "storePassword" : {
      "title" : "Store password secret ID",
      "description" : "The secret ID from which the store password can be obtained, or none if
 the password is blank. This secret ID will be resolved using one of the other secret stores
 configured.<br> It must not start or end with the <code>.</code> character <br>The <code>.</code>
 character must not be followed by another <code>.</code> character.<br>Must contain <code>a-z</code>,
 <code>A-Z</code>, <code>0-9</code> and <code>.</code> characters only.",
      "propertyOrder" : 400,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
    },
    "storetype" : {
      "title" : "Keystore type",
      "description" : "The type of the keystore (JKS, JCEKS, PKCS11, PKCS12, others). This must be a
 keystore type known or configured on the JRE.",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "leaseExpiryDuration" : {
      "title" : "Key lease expiry",
      "description" : "The amount of minutes a key can be cached from the keystore before it needs to
 be reloaded.",
      "propertyOrder" : 600,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "providerName" : {
      "title" : "Provider name",
      "description" : "The classname of a provider to use to load the keystore. If blank, the JRE
 default will be used.",
      "propertyOrder" : 300,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
    },
    "keyEntryPassword" : {
      "title" : "Entry password secret ID",
      "description" : "The secret value from which the entry password can be obtained, or none
 if the password is blank. This secret ID will be resolved using one of the other secret stores
 configured.<br> It must not start or end with the <code>.</code> character. <br>The <code>.</code>
```

```
 character must not be followed by another <code>.</code> character.<br>Must contain <code>a-z</code>,
 <code>A-Z</code>, <code>0-9</code> and <code>.</code> characters only.",
      "propertyOrder" : 500,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
```

LDAPDecision

Realm Operations

Resource path: `/realm-config/authentication/authenticationtrees/nodes/LdapDecisionNode`

Resource version: `1.0`

create

Usage:

```
am> create LDAPDecision --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "secondaryServers" : {
      "title" : "Secondary LDAP Server",
      "description" : "Specify one or more secondary directory servers. <br><br>Specify
 each directory server in the following format: <br><code>host:port</code><br><br>Secondary
 servers are used when none of the primary servers are available.<br><br>For example,
 <code>directory_services_backup.example.com</code>.",
      "propertyOrder" : 200,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "trustAllServerCertificates" : {
```

```
      "title" : "Trust All Server Certificates",
      "description" : "When enabled, blindly trust server certificates, including self-signed test
 certificates. <br><br><em>Note:</em> Use this feature with care as it bypasses the normal certificate
 verification process.",
      "propertyOrder" : 1500,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "returnUserDn" : {
      "title" : "Return User DN to DataStore",
      "description" : "When enabled, the node returns the DN rather than the User ID.",
      "propertyOrder" : 1100,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "ldapConnectionMode" : {
      "title" : "LDAP Connection Mode",
      "description" : "Specifies whether to use SSL or StartTLS to connect to the LDAP user data
 store.  <br><br>AM must be able to trust the certificates used.",
      "propertyOrder" : 1000,
      "type" : "string",
      "exampleValue" : ""
    },
    "userSearchFilter" : {
      "title" : "User Search Filter",
      "description" : "Specifies an additional filter to append to user searches.
 <br><br>For example, searching for <code>mail</code> and specifying a User Search Filter of
 <code>(objectClass=inetOrgPerson)</code>, causes AM to use <code>(&amp;(mail=<replaceable>address</
replaceable>)(objectClass=inetOrgPerson))</code> as the resulting search filter, where
 <replaceable>address</replaceable> is the mail address provided by the user.",
      "propertyOrder" : 800,
      "type" : "string",
      "exampleValue" : ""
    },
    "beheraEnabled" : {
      "title" : "LDAP Behera Password Policy Support",
      "description" : "Enables support for modern LDAP password policies. <br><br>LDAP Behera Password
 policies are supported by modern LDAP servers such as DS. If this functionality is disabled then only
 the older Netscape VCHU password policy standard will be enforced.",
      "propertyOrder" : 1400,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "heartbeatInterval" : {
      "title" : "LDAP Connection Heartbeat Interval",
      "description" : "Specifies how often AM should send a heartbeat request to the directory server
 to ensure that the connection does not remain idle. <br><br>Some network administrators configure
 firewalls and load balancers to drop connections that are idle for too long. You can turn this off
 by setting the value to <code>0</code> or to a negative number. Set the units for the interval in the
 LDAP Connection Heartbeat Time Unit property.",
      "propertyOrder" : 1600,
      "type" : "integer",
      "exampleValue" : ""
    },
    "searchScope" : {
      "title" : "Search Scope",
      "description" : "Specifies the extent of searching for users in the directory server.
 <br><br>Scope <code>OBJECT</code> means search only the entry specified as the DN to Start User
```

```
Search, whereas <code>ONELEVEL</code> means search only the entries that are directly children of
that object. <code>SUBTREE</code> means search the entry specified and every entry under it.",
     "propertyOrder" : 900,
     "type" : "string",
     "exampleValue" : ""
   },
   "accountSearchBaseDn" : {
     "title" : "DN to Start User Search",
     "description" : "Specify the DN from which to start the user search.<br><br>More specific DNs,
such as <code>ou=sales,dc=example,dc=com</code>, result in better search performance.If multiple
entries exist in the store with identical attribute values, ensure this property is specific enough
to return only one entry.",
     "propertyOrder" : 300,
     "items" : {
       "type" : "string"
     },
     "minItems" : 1,
     "type" : "array",
     "exampleValue" : ""
   },
   "adminPassword" : {
     "title" : "Bind User Password",
     "description" : "Specify the password of the account used to bind to the LDAP user data store.",
     "propertyOrder" : 500,
     "type" : "string",
     "format" : "password",
     "exampleValue" : ""
   },
   "userProfileAttribute" : {
     "title" : "Attribute Used to Retrieve User Profile",
     "description" : "Specifies the attribute used to retrieve the profile of a user from the
directory server. <br><br>The user search will have already happened, as specified by the Attributes
Used to Search for a User to be Authenticated and User Search Filter properties.",
     "propertyOrder" : 600,
     "type" : "string",
     "exampleValue" : ""
   },
   "heartbeatTimeUnit" : {
     "title" : "LDAP Connection Heartbeat Time Unit",
     "description" : "Specifies the time unit corresponding to LDAP Connection Heartbeat
Interval.<br><br> Default: Seconds",
     "propertyOrder" : 1700,
     "type" : "string",
     "exampleValue" : ""
   },
   "adminDn" : {
     "title" : "Bind User DN",
     "description" : "Specify the user DN used to bind to the LDAP user data store.
<br><br><em>Note:</em> <code>cn=Directory Manager</code> should not be used in production systems.",
     "propertyOrder" : 400,
     "type" : "string",
     "exampleValue" : ""
   },
   "ldapOperationsTimeout" : {
     "title" : "LDAP Operations Timeout",
     "description" : "Defines the timeout in milliseconds that AM should wait for a response from the
directory server.<br><br> Default: <code>0</code> (No timeout).",
     "propertyOrder" : 1800,
     "type" : "integer",
```

```
      "exampleValue" : ""
    },
    "userCreationAttrs" : {
      "title" : "User Creation Attributes",
      "description" : "This list lets you map (external) attribute names from the LDAP directory
 server to (internal) attribute names used by AM. <br><br>The format of this property is:
 <br><code>local attr1|external attr1</code>",
      "propertyOrder" : 1200,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "searchFilterAttributes" : {
      "title" : "Attributes Used to Search for a User to be Authenticated",
      "description" : "Specifies the attributes used to match an entry in the directory server to
 the credentials provided by the user. <br><br>The default value of <code>uid</code> will form the
 following search filter of <code>uid=user</code>. Specifying multiple values such as <code>uid</
code> and <code>cn</code> causes the node to create a search filter of <code>(|(uid=user)(cn=user))</
code>. <br><br>Multiple attribute values allow the user to authenticate with any one of the values.
 For example, if you have both <code>uid</code> and <code>mail</code>, then Barbara Jensen can
 authenticate with either <code>bjensen</code> or <code>bjensen@example.com</code>.",
      "propertyOrder" : 700,
      "items" : {
        "type" : "string"
      },
      "minItems" : 1,
      "type" : "array",
      "exampleValue" : ""
    },
    "minimumPasswordLength" : {
      "title" : "Minimum Password Length",
      "description" : "Specifies the minimum acceptable password length.",
      "propertyOrder" : 1300,
      "type" : "integer",
      "exampleValue" : ""
    },
    "primaryServers" : {
      "title" : "Primary LDAP Server",
      "description" : "Specify one or more primary directory servers. <br><br>Specify each
 directory server in the following format: <br><code>host:port</code><br><br>For example,
 <code>directory_services.example.com:389</code>.",
      "propertyOrder" : 100,
      "items" : {
        "type" : "string"
      },
      "minItems" : 1,
      "type" : "array",
      "exampleValue" : ""
    }
  },
  "required" : [ "trustAllServerCertificates", "searchFilterAttributes", "heartbeatInterval",
 "searchScope", "returnUserDn", "beheraEnabled", "ldapConnectionMode", "secondaryServers",
 "accountSearchBaseDn", "primaryServers", "adminPassword", "adminDn", "ldapOperationsTimeout",
 "userProfileAttribute", "userCreationAttrs", "minimumPasswordLength", "heartbeatTimeUnit" ]
}
```

delete

Usage:

```
am> delete LDAPDecision --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action LDAPDecision --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action LDAPDecision --realm Realm --actionName getCreatableTypes
```

listOutcomes

List the available outcomes for the node type.

Usage:

```
am> action LDAPDecision --realm Realm --body body --actionName listOutcomes
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "title" : "Some configuration of the node. This does not need to be complete against the
 configuration schema."
}
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action LDAPDecision --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query LDAPDecision --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read LDAPDecision --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update LDAPDecision --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "secondaryServers" : {
      "title" : "Secondary LDAP Server",
      "description" : "Specify one or more secondary directory servers. <br><br>Specify
 each directory server in the following format: <br><code>host:port</code><br><br>Secondary
 servers are used when none of the primary servers are available.<br><br>For example,
 <code>directory_services_backup.example.com</code>.",
      "propertyOrder" : 200,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "trustAllServerCertificates" : {
      "title" : "Trust All Server Certificates",
      "description" : "When enabled, blindly trust server certificates, including self-signed test
 certificates. <br><br><em>Note:</em> Use this feature with care as it bypasses the normal certificate
 verification process.",
      "propertyOrder" : 1500,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "returnUserDn" : {
      "title" : "Return User DN to DataStore",
      "description" : "When enabled, the node returns the DN rather than the User ID.",
      "propertyOrder" : 1100,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "ldapConnectionMode" : {
      "title" : "LDAP Connection Mode",
      "description" : "Specifies whether to use SSL or StartTLS to connect to the LDAP user data
 store.  <br><br>AM must be able to trust the certificates used.",
      "propertyOrder" : 1000,
      "type" : "string",
      "exampleValue" : ""
    },
    "userSearchFilter" : {
      "title" : "User Search Filter",
      "description" : "Specifies an additional filter to append to user searches.
 <br><br>For example, searching for <code>mail</code> and specifying a User Search Filter of
 <code>(objectClass=inetOrgPerson)</code>, causes AM to use <code>(&amp;(mail=<replaceable>address</
replaceable>)(objectClass=inetOrgPerson))</code> as the resulting search filter, where
 <replaceable>address</replaceable> is the mail address provided by the user.",
      "propertyOrder" : 800,
      "type" : "string",
      "exampleValue" : ""
    },
    "beheraEnabled" : {
      "title" : "LDAP Behera Password Policy Support",
```

```
     "description" : "Enables support for modern LDAP password policies. <br><br>LDAP Behera Password
policies are supported by modern LDAP servers such as DS. If this functionality is disabled then only
the older Netscape VCHU password policy standard will be enforced.",
     "propertyOrder" : 1400,
     "type" : "boolean",
     "exampleValue" : ""
   },
   "heartbeatInterval" : {
     "title" : "LDAP Connection Heartbeat Interval",
     "description" : "Specifies how often AM should send a heartbeat request to the directory server
to ensure that the connection does not remain idle. <br><br>Some network administrators configure
firewalls and load balancers to drop connections that are idle for too long. You can turn this off
by setting the value to <code>0</code> or to a negative number. Set the units for the interval in the
LDAP Connection Heartbeat Time Unit property.",
     "propertyOrder" : 1600,
     "type" : "integer",
     "exampleValue" : ""
   },
   "searchScope" : {
     "title" : "Search Scope",
     "description" : "Specifies the extent of searching for users in the directory server.
<br><br>Scope <code>OBJECT</code> means search only the entry specified as the DN to Start User
Search, whereas <code>ONELEVEL</code> means search only the entries that are directly children of
that object. <code>SUBTREE</code> means search the entry specified and every entry under it.",
     "propertyOrder" : 900,
     "type" : "string",
     "exampleValue" : ""
   },
   "accountSearchBaseDn" : {
     "title" : "DN to Start User Search",
     "description" : "Specify the DN from which to start the user search.<br><br>More specific DNs,
such as <code>ou=sales,dc=example,dc=com</code>, result in better search performance.If multiple
entries exist in the store with identical attribute values, ensure this property is specific enough
to return only one entry.",
     "propertyOrder" : 300,
     "items" : {
       "type" : "string"
     },
     "minItems" : 1,
     "type" : "array",
     "exampleValue" : ""
   },
   "adminPassword" : {
     "title" : "Bind User Password",
     "description" : "Specify the password of the account used to bind to the LDAP user data store.",
     "propertyOrder" : 500,
     "type" : "string",
     "format" : "password",
     "exampleValue" : ""
   },
   "userProfileAttribute" : {
     "title" : "Attribute Used to Retrieve User Profile",
     "description" : "Specifies the attribute used to retrieve the profile of a user from the
directory server. <br><br>The user search will have already happened, as specified by the Attributes
Used to Search for a User to be Authenticated and User Search Filter properties.",
     "propertyOrder" : 600,
     "type" : "string",
     "exampleValue" : ""
   },
```

```
    "heartbeatTimeUnit" : {
      "title" : "LDAP Connection Heartbeat Time Unit",
      "description" : "Specifies the time unit corresponding to LDAP Connection Heartbeat
 Interval.<br><br> Default: Seconds",
      "propertyOrder" : 1700,
      "type" : "string",
      "exampleValue" : ""
    },
    "adminDn" : {
      "title" : "Bind User DN",
      "description" : "Specify the user DN used to bind to the LDAP user data store.
 <br><br><em>Note:</em> <code>cn=Directory Manager</code> should not be used in production systems.",
      "propertyOrder" : 400,
      "type" : "string",
      "exampleValue" : ""
    },
    "ldapOperationsTimeout" : {
      "title" : "LDAP Operations Timeout",
      "description" : "Defines the timeout in milliseconds that AM should wait for a response from the
 directory server.<br><br> Default: <code>0</code> (No timeout).",
      "propertyOrder" : 1800,
      "type" : "integer",
      "exampleValue" : ""
    },
    "userCreationAttrs" : {
      "title" : "User Creation Attributes",
      "description" : "This list lets you map (external) attribute names from the LDAP directory
 server to (internal) attribute names used by AM. <br><br>The format of this property is:
 <br><code>local attr1|external attr1</code>",
      "propertyOrder" : 1200,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "searchFilterAttributes" : {
      "title" : "Attributes Used to Search for a User to be Authenticated",
      "description" : "Specifies the attributes used to match an entry in the directory server to
 the credentials provided by the user. <br><br>The default value of <code>uid</code> will form the
 following search filter of <code>uid=user</code>. Specifying multiple values such as <code>uid</
code> and <code>cn</code> causes the node to create a search filter of <code>(|(uid=user)(cn=user))</
code>. <br><br>Multiple attribute values allow the user to authenticate with any one of the values.
 For example, if you have both <code>uid</code> and <code>mail</code>, then Barbara Jensen can
 authenticate with either <code>bjensen</code> or <code>bjensen@example.com</code>.",
      "propertyOrder" : 700,
      "items" : {
        "type" : "string"
      },
      "minItems" : 1,
      "type" : "array",
      "exampleValue" : ""
    },
    "minimumPasswordLength" : {
      "title" : "Minimum Password Length",
      "description" : "Specifies the minimum acceptable password length.",
      "propertyOrder" : 1300,
      "type" : "integer",
      "exampleValue" : ""
```

```
    },
    "primaryServers" : {
      "title" : "Primary LDAP Server",
      "description" : "Specify one or more primary directory servers. <br><br>Specify each
 directory server in the following format: <br><code>host:port</code><br><br>For example,
 <code>directory_services.example.com:389</code>.",
      "propertyOrder" : 100,
      "items" : {
        "type" : "string"
      },
      "minItems" : 1,
      "type" : "array",
      "exampleValue" : ""
    }
  },
  "required" : [ "trustAllServerCertificates", "searchFilterAttributes", "heartbeatInterval",
 "searchScope", "returnUserDn", "beheraEnabled", "ldapConnectionMode", "secondaryServers",
 "accountSearchBaseDn", "primaryServers", "adminPassword", "adminDn", "ldapOperationsTimeout",
 "userProfileAttribute", "userCreationAttrs", "minimumPasswordLength", "heartbeatTimeUnit" ]
}
```

LdapModule

Realm Operations

Resource path: `/realm-config/authentication/modules/ldap`

Resource version: `1.0`

create

Usage:

```
am> create LdapModule --realm Realm --id id --body body
```

Parameters:

`--id`

The unique identifier for the resource.

`--body`

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "userSearchStartDN" : {
      "title" : "DN to Start User Search",
```

```
      "description" : "The search for accounts to be authenticated start from this base DN <br><br>For
 a single server just enter the Base DN to be searched. Multiple OpenAM servers can have different
 base DNs for the search The format is as follows:<br/><br/><code>local server name | search DN</
code><br/><br/><i>NB </i>The local server name is the full name of the server from the list of servers
 and sites.",
      "propertyOrder" : 300,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "primaryLdapServer" : {
      "title" : "Primary LDAP Server",
      "description" : "Use this list to set the primary LDAP server used for authentication.
 <br><br>The LDAP authentication module will use this list as the primary server for authentication. A
 single entry must be in the format:<br/><br/><code>ldap_server:port</code><br/><br/>Multiple entries
 allow associations between OpenAM servers and a LDAP server. The format is:<br/><br/><code>local
 server name | server:port</code><br/><br/>The local server name is the full name of the server from
 the list of servers and sites.",
      "propertyOrder" : 100,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "authenticationLevel" : {
      "title" : "Authentication Level",
      "description" : "The authentication level associated with this module.<br><br>Each
 authentication module has an authentication level that can be used to indicate the level of security
 associated with the module; 0 is the lowest (and the default). ",
      "propertyOrder" : 2000,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "searchScope" : {
      "title" : "Search Scope",
      "description" : "The level in the Directory Server that will be searched for a matching
 user profile.<br><br>This attribute controls how the directory is searched.<br/><br/
><ul><li><code>OBJECT</code>: Only the Base DN is searched.</li><li><code>ONELEVEL</code>: Only the
 single level below (and not the Base DN) is searched</li><li><code>SUBTREE</code>: The Base DN and
 all levels below are searched</li></ul>",
      "propertyOrder" : 900,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "returnUserDN" : {
      "title" : "Return User DN to DataStore",
      "description" : "Controls whether the DN or the username is returned as the authentication
 principal.",
      "propertyOrder" : 1200,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
```

```
    },
    "beheraPasswordPolicySupportEnabled" : {
      "title" : "LDAP Behera Password Policy Support",
      "description" : "Enables support for modern LDAP password policies<br><br>LDAP Behera Password
 policies are supported by modern LDAP servers such as OpenDJ. If this functionality is disabled then
 only the older Netscape VCHU password policy standard will be enforced.",
      "propertyOrder" : 1500,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "userSearchAttributes" : {
      "title" : "Attributes Used to Search for a User to be Authenticated",
      "description" : "The attributes specified in this list form the LDAP search filter.<br><br>The
 default value of uid will form the following search filter of <code>uid=<i>user</i></code>, if there
 are multiple values such as uid and cn, the module will create a search filter as follows <code>(|
(uid=<i>user</i>)(cn=<i>user</i>))</code>",
      "propertyOrder" : 700,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "userBindPassword" : {
      "title" : "Bind User Password",
      "description" : "The password of the administration account.",
      "propertyOrder" : 500,
      "required" : true,
      "type" : "string",
      "format" : "password",
      "exampleValue" : ""
    },
    "userBindDN" : {
      "title" : "Bind User DN",
      "description" : "The DN of an admin user used by the module to authentication to the LDAP
 server<br><br>The LDAP module requires an administration account in order to perform functionality
 such as password reset.<br/><br/><i>NB </i><code>cn=Directory Manager</code> should not be used in
 production systems.",
      "propertyOrder" : 400,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "minimumPasswordLength" : {
      "title" : "Minimum Password Length",
      "description" : "Enforced when the user is resetting their password as part of the
 authentication.<br><br>If the user needs to reset their password as part of the authentication
 process, the authentication module can enforce a minimum password length. This is separate from any
 password length controls from the underlying LDAP server. If the external LDAP server password policy
 is enforcing password length, set this value to 0 to avoid confusion.",
      "propertyOrder" : 1400,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "openam-auth-ldap-connection-mode" : {
      "title" : "LDAP Connection Mode",
```

```
      "description" : "Defines which protocol/operation is used to establish the connection to the
 LDAP Directory Server.<br><br>If 'LDAP' is selected, the connection <b>won't be secured</b> and
 passwords are transferred in <b>cleartext</b> over the network.<br/> If 'LDAPS' is selected, the
 connection is secured via SSL or TLS. <br/> If 'StartTLS' is selected, the connection is secured by
 using StartTLS extended operation.",
      "propertyOrder" : 1000,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "connectionHeartbeatTimeUnit" : {
      "title" : "LDAP Connection Heartbeat Time Unit",
      "description" : "Defines the time unit corresponding to the Heartbeat Interval
 setting.<br><br>This setting controls how often OpenAM <b>should</b> send a heartbeat search request
 to the configured directory. If a connection becomes unresponsive (e.g. due to a network error) then
 it may take up to the interval period before the problem is detected. Use along with the Heartbeat
 Interval parameter to define the exact interval.",
      "propertyOrder" : 1800,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "secondaryLdapServer" : {
      "title" : "Secondary LDAP Server",
      "description" : "Use this list to set the secondary (failover) LDAP server used for
 authentication.<br><br>If the primary LDAP server fails, the LDAP authentication module will failover
 to the secondary server. A single entry must be in the format:<br/><br/><code>ldap_server:port</
code><br/><br/>Multiple entries allow associations between OpenAM servers and a LDAP server. The
 format is:<br/><br/><code>local server name | server:port</code><br/><br/><i>NB </i>The local server
 name is the full name of the server from the list of servers and sites.",
      "propertyOrder" : 200,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "userProfileRetrievalAttribute" : {
      "title" : "Attribute Used to Retrieve User Profile",
      "description" : "The LDAP module will use this attribute to search of the profile of an
 authenticated user.<br><br>This is the attribute used to find the profile of the authenticated user.
 Normally this will be the same attribute used to find the user account. The value will be the name of
 the user used for authentication.",
      "propertyOrder" : 600,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "operationTimeout" : {
      "title" : "LDAP operations timeout",
      "description" : "Defines the timeout in seconds OpenAM should wait for a response of the
 Directory Server - <code>0</code> means no timeout.<br><br>If the Directory Server's host is down
 completely or the TCP connection became stale OpenAM waits until operation timeouts from the OS or
 the JVM are applied. However this setting allows more granular control within OpenAM itself. A value
 of <code>0</code> means NO timeout is applied on OpenAM level and the timeouts from the JVM or OS
 will apply.",
      "propertyOrder" : 1900,
      "required" : true,
```

```
      "type" : "integer",
      "exampleValue" : ""
    },
    "profileAttributeMappings" : {
      "title" : "User Creation Attributes",
      "description" : "Controls the mapping of local attribute to external attribute for dynamic
 profile creation.<br><br>If dynamic profile creation is enabled; this feature allows for a mapping
 between the attribute/values retrieved from the users authenticated profile and the attribute/values
 that will be provisioned into their matching account in the data store.<br/><br/>The format of this
 property is: <br/><br/><code> local attr1|external attr1</code>",
      "propertyOrder" : 1300,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "connectionHeartbeatInterval" : {
      "title" : "LDAP Connection Heartbeat Interval",
      "description" : "Specifies how often should OpenAM send a heartbeat request to the
 directory.<br><br>This setting controls how often OpenAM <b>should</b> send a heartbeat search
 request to the configured directory. If a connection becomes unresponsive (e.g. due to a network
 error) then it may take up to the interval period before the problem is detected. Use along with the
 Heartbeat Time Unit parameter to define the exact interval. Zero or negative value will result in
 disabling heartbeat requests.",
      "propertyOrder" : 1700,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "userSearchFilter" : {
      "title" : "User Search Filter",
      "description" : "This search filter will be appended to the standard user search
 filter.<br><br>This attribute can be used to append a custom search filter to the standard filter.
 For example: <code>(objectClass=person)</code>would result in the following user search filter:<br/
><br/><code>(&(uid=<i>user</i>)(objectClass=person))</code>",
      "propertyOrder" : 800,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "trustAllServerCertificates" : {
      "title" : "Trust All Server Certificates",
      "description" : "Enables a <code>X509TrustManager</code> that trusts all
 certificates.<br><br>This feature will allow the LDAP authentication module to connect to LDAP
 servers protected by self signed or invalid certificates (such as invalid hostname).<br/><br/><i>NB
 </i>Use this feature with care as it bypasses the normal certificate verification process",
      "propertyOrder" : 1600,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    }
  }
}
```

delete

Usage:

```
am> delete LdapModule --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action LdapModule --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action LdapModule --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action LdapModule --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query LdapModule --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read LdapModule --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update LdapModule --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "userSearchStartDN" : {
      "title" : "DN to Start User Search",
      "description" : "The search for accounts to be authenticated start from this base DN <br><br>For
 a single server just enter the Base DN to be searched. Multiple OpenAM servers can have different
 base DNs for the search The format is as follows:<br/><br/><code>local server name | search DN</
code><br/><br/><i>NB </i>The local server name is the full name of the server from the list of servers
 and sites.",
      "propertyOrder" : 300,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "primaryLdapServer" : {
      "title" : "Primary LDAP Server",
      "description" : "Use this list to set the primary LDAP server used for authentication.
 <br><br>The LDAP authentication module will use this list as the primary server for authentication. A
 single entry must be in the format:<br/><br/><code>ldap_server:port</code><br/><br/>Multiple entries
 allow associations between OpenAM servers and a LDAP server. The format is:<br/><br/><code>local
 server name | server:port</code><br/><br/>The local server name is the full name of the server from
 the list of servers and sites.",
      "propertyOrder" : 100,
```

```
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "authenticationLevel" : {
      "title" : "Authentication Level",
      "description" : "The authentication level associated with this module.<br><br>Each
 authentication module has an authentication level that can be used to indicate the level of security
 associated with the module; 0 is the lowest (and the default). ",
      "propertyOrder" : 2000,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "searchScope" : {
      "title" : "Search Scope",
      "description" : "The level in the Directory Server that will be searched for a matching
 user profile.<br><br>This attribute controls how the directory is searched.<br/><br/
><ul><li><code>OBJECT</code>: Only the Base DN is searched.</li><li><code>ONELEVEL</code>: Only the
 single level below (and not the Base DN) is searched</li><li><code>SUBTREE</code>: The Base DN and
 all levels below are searched</li></ul>",
      "propertyOrder" : 900,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "returnUserDN" : {
      "title" : "Return User DN to DataStore",
      "description" : "Controls whether the DN or the username is returned as the authentication
 principal.",
      "propertyOrder" : 1200,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "beheraPasswordPolicySupportEnabled" : {
      "title" : "LDAP Behera Password Policy Support",
      "description" : "Enables support for modern LDAP password policies<br><br>LDAP Behera Password
 policies are supported by modern LDAP servers such as OpenDJ. If this functionality is disabled then
 only the older Netscape VCHU password policy standard will be enforced.",
      "propertyOrder" : 1500,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "userSearchAttributes" : {
      "title" : "Attributes Used to Search for a User to be Authenticated",
      "description" : "The attributes specified in this list form the LDAP search filter.<br><br>The
 default value of uid will form the following search filter of <code>uid=<i>user</i></code>, if there
 are multiple values such as uid and cn, the module will create a search filter as follows <code>(|
(uid=<i>user</i>)(cn=<i>user</i>))</code>",
      "propertyOrder" : 700,
      "required" : true,
      "items" : {
        "type" : "string"
      },
```

```
      "type" : "array",
      "exampleValue" : ""
    },
    "userBindPassword" : {
      "title" : "Bind User Password",
      "description" : "The password of the administration account.",
      "propertyOrder" : 500,
      "required" : true,
      "type" : "string",
      "format" : "password",
      "exampleValue" : ""
    },
    "userBindDN" : {
      "title" : "Bind User DN",
      "description" : "The DN of an admin user used by the module to authentication to the LDAP
server<br><br>The LDAP module requires an administration account in order to perform functionality
such as password reset.<br/><br/><i>NB </i><code>cn=Directory Manager</code> should not be used in
production systems.",
      "propertyOrder" : 400,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "minimumPasswordLength" : {
      "title" : "Minimum Password Length",
      "description" : "Enforced when the user is resetting their password as part of the
authentication.<br><br>If the user needs to reset their password as part of the authentication
process, the authentication module can enforce a minimum password length. This is separate from any
password length controls from the underlying LDAP server. If the external LDAP server password policy
is enforcing password length, set this value to 0 to avoid confusion.",
      "propertyOrder" : 1400,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "openam-auth-ldap-connection-mode" : {
      "title" : "LDAP Connection Mode",
      "description" : "Defines which protocol/operation is used to establish the connection to the
LDAP Directory Server.<br><br>If 'LDAP' is selected, the connection <b>won't be secured</b> and
passwords are transferred in <b>cleartext</b> over the network.<br/> If 'LDAPS' is selected, the
connection is secured via SSL or TLS. <br/> If 'StartTLS' is selected, the connection is secured by
using StartTLS extended operation.",
      "propertyOrder" : 1000,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "connectionHeartbeatTimeUnit" : {
      "title" : "LDAP Connection Heartbeat Time Unit",
      "description" : "Defines the time unit corresponding to the Heartbeat Interval
setting.<br><br>This setting controls how often OpenAM <b>should</b> send a heartbeat search request
to the configured directory. If a connection becomes unresponsive (e.g. due to a network error) then
it may take up to the interval period before the problem is detected. Use along with the Heartbeat
Interval parameter to define the exact interval.",
      "propertyOrder" : 1800,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
```

```
    "secondaryLdapServer" : {
      "title" : "Secondary LDAP Server",
      "description" : "Use this list to set the secondary (failover) LDAP server used for
 authentication.<br><br>If the primary LDAP server fails, the LDAP authentication module will failover
 to the secondary server. A single entry must be in the format:<br/><br/><code>ldap_server:port</
code><br/><br/>Multiple entries allow associations between OpenAM servers and a LDAP server. The
 format is:<br/><br/><code>local server name | server:port</code><br/><br/><i>NB </i>The local server
 name is the full name of the server from the list of servers and sites.",
      "propertyOrder" : 200,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "userProfileRetrievalAttribute" : {
      "title" : "Attribute Used to Retrieve User Profile",
      "description" : "The LDAP module will use this attribute to search of the profile of an
 authenticated user.<br><br>This is the attribute used to find the profile of the authenticated user.
 Normally this will be the same attribute used to find the user account. The value will be the name of
 the user used for authentication.",
      "propertyOrder" : 600,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "operationTimeout" : {
      "title" : "LDAP operations timeout",
      "description" : "Defines the timeout in seconds OpenAM should wait for a response of the
 Directory Server - <code>0</code> means no timeout.<br><br>If the Directory Server's host is down
 completely or the TCP connection became stale OpenAM waits until operation timeouts from the OS or
 the JVM are applied. However this setting allows more granular control within OpenAM itself. A value
 of <code>0</code> means NO timeout is applied on OpenAM level and the timeouts from the JVM or OS
 will apply.",
      "propertyOrder" : 1900,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "profileAttributeMappings" : {
      "title" : "User Creation Attributes",
      "description" : "Controls the mapping of local attribute to external attribute for dynamic
 profile creation.<br><br>If dynamic profile creation is enabled; this feature allows for a mapping
 between the attribute/values retrieved from the users authenticated profile and the attribute/values
 that will be provisioned into their matching account in the data store.<br/><br/>The format of this
 property is: <br/><br/><code> local attr1|external attr1</code>",
      "propertyOrder" : 1300,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "connectionHeartbeatInterval" : {
      "title" : "LDAP Connection Heartbeat Interval",
      "description" : "Specifies how often should OpenAM send a heartbeat request to the
 directory.<br><br>This setting controls how often OpenAM <b>should</b> send a heartbeat search
```

```
 request to the configured directory. If a connection becomes unresponsive (e.g. due to a network
 error) then it may take up to the interval period before the problem is detected. Use along with the
 Heartbeat Time Unit parameter to define the exact interval. Zero or negative value will result in
 disabling heartbeat requests.",
      "propertyOrder" : 1700,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "userSearchFilter" : {
      "title" : "User Search Filter",
      "description" : "This search filter will be appended to the standard user search
 filter.<br><br>This attribute can be used to append a custom search filter to the standard filter.
 For example: <code>(objectClass=person)</code>would result in the following user search filter:<br/
><br/><code>(&(uid=<i>user</i>)(objectClass=person))</code>",
      "propertyOrder" : 800,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "trustAllServerCertificates" : {
      "title" : "Trust All Server Certificates",
      "description" : "Enables a <code>X509TrustManager</code> that trusts all
 certificates.<br><br>This feature will allow the LDAP authentication module to connect to LDAP
 servers protected by self signed or invalid certificates (such as invalid hostname).<br/><br/><i>NB
 </i>Use this feature with care as it bypasses the normal certificate verification process",
      "propertyOrder" : 1600,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    }
  }
}
```


Global Operations

Resource path: `/global-config/authentication/modules/ldap`

Resource version: `1.0`

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action LdapModule --global --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action LdapModule --global --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action LdapModule --global --actionName nextdescendents
```

read

Usage:

```
am> read LdapModule --global
```

update

Usage:

```
am> update LdapModule --global --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "defaults" : {
      "properties" : {
        "minimumPasswordLength" : {
          "title" : "Minimum Password Length",
          "description" : "Enforced when the user is resetting their password as part of the
 authentication.<br><br>If the user needs to reset their password as part of the authentication
 process, the authentication module can enforce a minimum password length. This is separate from any
 password length controls from the underlying LDAP server. If the external LDAP server password policy
 is enforcing password length, set this value to 0 to avoid confusion.",
          "propertyOrder" : 1400,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "openam-auth-ldap-connection-mode" : {
          "title" : "LDAP Connection Mode",
          "description" : "Defines which protocol/operation is used to establish the connection to
 the LDAP Directory Server.<br><br>If 'LDAP' is selected, the connection <b>won't be secured</b> and
 passwords are transferred in <b>cleartext</b> over the network.<br/> If 'LDAPS' is selected, the
 connection is secured via SSL or TLS. <br/> If 'StartTLS' is selected, the connection is secured by
 using StartTLS extended operation.",
          "propertyOrder" : 1000,
```

```
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "searchScope" : {
          "title" : "Search Scope",
          "description" : "The level in the Directory Server that will be searched for a
 matching user profile.<br><br>This attribute controls how the directory is searched.<br/><br/
><ul><li><code>OBJECT</code>: Only the Base DN is searched.</li><li><code>ONELEVEL</code>: Only the
 single level below (and not the Base DN) is searched</li><li><code>SUBTREE</code>: The Base DN and
 all levels below are searched</li></ul>",
          "propertyOrder" : 900,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "operationTimeout" : {
          "title" : "LDAP operations timeout",
          "description" : "Defines the timeout in seconds OpenAM should wait for a response of the
 Directory Server - <code>0</code> means no timeout.<br><br>If the Directory Server's host is down
 completely or the TCP connection became stale OpenAM waits until operation timeouts from the OS or
 the JVM are applied. However this setting allows more granular control within OpenAM itself. A value
 of <code>0</code> means NO timeout is applied on OpenAM level and the timeouts from the JVM or OS
 will apply.",
          "propertyOrder" : 1900,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "userBindDN" : {
          "title" : "Bind User DN",
          "description" : "The DN of an admin user used by the module to authentication to the LDAP
 server<br><br>The LDAP module requires an administration account in order to perform functionality
 such as password reset.<br/><br/><i>NB </i><code>cn=Directory Manager</code> should not be used in
 production systems.",
          "propertyOrder" : 400,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "userProfileRetrievalAttribute" : {
          "title" : "Attribute Used to Retrieve User Profile",
          "description" : "The LDAP module will use this attribute to search of the profile of an
 authenticated user.<br><br>This is the attribute used to find the profile of the authenticated user.
 Normally this will be the same attribute used to find the user account. The value will be the name of
 the user used for authentication.",
          "propertyOrder" : 600,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "userSearchAttributes" : {
          "title" : "Attributes Used to Search for a User to be Authenticated",
          "description" : "The attributes specified in this list form the LDAP search
 filter.<br><br>The default value of uid will form the following search filter of <code>uid=<i>user</
i></code>, if there are multiple values such as uid and cn, the module will create a search filter as
 follows <code>(|(uid=<i>user</i>)(cn=<i>user</i>))</code>",
          "propertyOrder" : 700,
          "required" : true,
```

```
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "returnUserDN" : {
          "title" : "Return User DN to DataStore",
          "description" : "Controls whether the DN or the username is returned as the authentication
principal.",
          "propertyOrder" : 1200,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "profileAttributeMappings" : {
          "title" : "User Creation Attributes",
          "description" : "Controls the mapping of local attribute to external attribute for dynamic
profile creation.<br><br>If dynamic profile creation is enabled; this feature allows for a mapping
between the attribute/values retrieved from the users authenticated profile and the attribute/values
that will be provisioned into their matching account in the data store.<br/><br/>The format of this
property is: <br/><br/><code> local attr1|external attr1</code>",
          "propertyOrder" : 1300,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "beheraPasswordPolicySupportEnabled" : {
          "title" : "LDAP Behera Password Policy Support",
          "description" : "Enables support for modern LDAP password policies<br><br>LDAP Behera
Password policies are supported by modern LDAP servers such as OpenDJ. If this functionality is
disabled then only the older Netscape VCHU password policy standard will be enforced.",
          "propertyOrder" : 1500,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "userBindPassword" : {
          "title" : "Bind User Password",
          "description" : "The password of the administration account.",
          "propertyOrder" : 500,
          "required" : true,
          "type" : "string",
          "format" : "password",
          "exampleValue" : ""
        },
        "trustAllServerCertificates" : {
          "title" : "Trust All Server Certificates",
          "description" : "Enables a <code>X509TrustManager</code> that trusts all
certificates.<br><br>This feature will allow the LDAP authentication module to connect to LDAP
servers protected by self signed or invalid certificates (such as invalid hostname).<br/><br/><i>NB
</i>Use this feature with care as it bypasses the normal certificate verification process",
          "propertyOrder" : 1600,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
```

```
        },
        "authenticationLevel" : {
          "title" : "Authentication Level",
          "description" : "The authentication level associated with this module.<br><br>Each
 authentication module has an authentication level that can be used to indicate the level of security
 associated with the module; 0 is the lowest (and the default). ",
          "propertyOrder" : 2000,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "connectionHeartbeatInterval" : {
          "title" : "LDAP Connection Heartbeat Interval",
          "description" : "Specifies how often should OpenAM send a heartbeat request to the
 directory.<br><br>This setting controls how often OpenAM <b>should</b> send a heartbeat search
 request to the configured directory. If a connection becomes unresponsive (e.g. due to a network
 error) then it may take up to the interval period before the problem is detected. Use along with the
 Heartbeat Time Unit parameter to define the exact interval. Zero or negative value will result in
 disabling heartbeat requests.",
          "propertyOrder" : 1700,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "secondaryLdapServer" : {
          "title" : "Secondary LDAP Server",
          "description" : "Use this list to set the secondary (failover) LDAP server used for
 authentication.<br><br>If the primary LDAP server fails, the LDAP authentication module will failover
 to the secondary server. A single entry must be in the format:<br/><br/><code>ldap_server:port</
code><br/><br/>Multiple entries allow associations between OpenAM servers and a LDAP server. The
 format is:<br/><br/><code>local server name | server:port</code><br/><br/><i>NB </i>The local server
 name is the full name of the server from the list of servers and sites.",
          "propertyOrder" : 200,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "connectionHeartbeatTimeUnit" : {
          "title" : "LDAP Connection Heartbeat Time Unit",
          "description" : "Defines the time unit corresponding to the Heartbeat Interval
 setting.<br><br>This setting controls how often OpenAM <b>should</b> send a heartbeat search request
 to the configured directory. If a connection becomes unresponsive (e.g. due to a network error) then
 it may take up to the interval period before the problem is detected. Use along with the Heartbeat
 Interval parameter to define the exact interval.",
          "propertyOrder" : 1800,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "primaryLdapServer" : {
          "title" : "Primary LDAP Server",
          "description" : "Use this list to set the primary LDAP server used for authentication.
 <br><br>The LDAP authentication module will use this list as the primary server for authentication. A
 single entry must be in the format:<br/><br/><code>ldap_server:port</code><br/><br/>Multiple entries
 allow associations between OpenAM servers and a LDAP server. The format is:<br/><br/><code>local
```

```
 server name | server:port</code><br/><br/>The local server name is the full name of the server from
 the list of servers and sites.",
          "propertyOrder" : 100,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "userSearchFilter" : {
          "title" : "User Search Filter",
          "description" : "This search filter will be appended to the standard user search
 filter.<br><br>This attribute can be used to append a custom search filter to the standard filter.
 For example: <code>(objectClass=person)</code>would result in the following user search filter:<br/
><br/><code>(&(uid=<i>user</i>)(objectClass=person))</code>",
          "propertyOrder" : 800,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "userSearchStartDN" : {
          "title" : "DN to Start User Search",
          "description" : "The search for accounts to be authenticated start from this base DN
 <br><br>For a single server just enter the Base DN to be searched. Multiple OpenAM servers can have
 different base DNs for the search The format is as follows:<br/><br/><code>local server name | search
 DN</code><br/><br/><i>NB </i>The local server name is the full name of the server from the list of
 servers and sites.",
          "propertyOrder" : 300,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        }
      },
      "type" : "object",
      "title" : "Realm Defaults"
    }
  }
}
```


LegacyUserSelfService

Realm Operations

Resource path: `/realm-config/services/security`

Resource version: `1.0`

create

Usage:

```
am> create LegacyUserSelfService --realm Realm --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "confirmationIdHmacKey" : {
      "title" : "Confirmation Id HMAC Signing Key",
      "description" : "256-bit key (base64-encoded) to use for HMAC signing of the legacy self-service
 confirmation email links.",
      "propertyOrder" : 1000,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "forgotPasswordEnabled" : {
      "title" : "Forgot Password for Users",
      "description" : "If enabled, users can assign themselves a new password using a REST API
 client.",
      "propertyOrder" : 500,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "userRegisteredDestination" : {
      "title" : "Destination After Successful Self-Registration",
      "description" : "Specifies the behavior when self-registration has successfully completed.",
      "propertyOrder" : 800,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "selfServiceEnabled" : {
      "title" : "Legacy Self-Service REST Endpoint",
      "description" : "Specify whether to enable the legacy self-service endpoint.<p>OpenAM supports
 two User Self-Service components: the Legacy User Self-Service, which is based on a Java SDK and is
 available in OpenAM versions prior to OpenAM 13, and a common REST-based/XUI-based User Self-Service
 available in OpenAM 13 and later.<p>The Legacy User Self-Service will be deprecated in a future
 release.",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "selfRegistrationEnabled" : {
      "title" : "Self-Registration for Users",
      "description" : "If enabled, new users can sign up using a REST API client.",
      "propertyOrder" : 200,
      "required" : true,
```

```
      "type" : "boolean",
      "exampleValue" : ""
    },
    "selfRegistrationConfirmationUrl" : {
      "title" : "Self-Registration Confirmation Email URL",
      "description" : "This page handles the HTTP GET request when the user clicks the link sent by
 email in the confirmation request.",
      "propertyOrder" : 400,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "forgotPasswordTokenLifetime" : {
      "title" : "Forgot Password Token Lifetime (seconds)",
      "description" : "Maximum life time for the token that allows a user to process a forgotten
 password using the REST API.",
      "propertyOrder" : 600,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "selfRegistrationTokenLifetime" : {
      "title" : "Self-Registration Token LifeTime (seconds)",
      "description" : "Maximum life time for the token allowing User Self-Registration using the REST
 API.",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "forgotPasswordConfirmationUrl" : {
      "title" : "Forgot Password Confirmation Email URL",
      "description" : "This page handles the HTTP GET request when the user clicks the link sent by
 email in the confirmation request.",
      "propertyOrder" : 700,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "protectedUserAttributes" : {
      "title" : "Protected User Attributes",
      "description" : "A list of user profile attributes. Users modifying any of the attributes in
 this list will be required to enter a password as confirmation before the change is accepted. This
 option applies to XUI deployments only.",
      "propertyOrder" : 900,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    }
  }
}
```

delete

Usage:

```
am> delete LegacyUserSelfService --realm Realm
```

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action LegacyUserSelfService --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action LegacyUserSelfService --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action LegacyUserSelfService --realm Realm --actionName nextdescendents
```

read

Usage:

```
am> read LegacyUserSelfService --realm Realm
```

update

Usage:

```
am> update LegacyUserSelfService --realm Realm --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "confirmationIdHmacKey" : {
      "title" : "Confirmation Id HMAC Signing Key",
```

```
     "description" : "256-bit key (base64-encoded) to use for HMAC signing of the legacy self-service
confirmation email links.",
     "propertyOrder" : 1000,
     "required" : true,
     "type" : "string",
     "exampleValue" : ""
   },
   "forgotPasswordEnabled" : {
     "title" : "Forgot Password for Users",
     "description" : "If enabled, users can assign themselves a new password using a REST API
client.",
     "propertyOrder" : 500,
     "required" : true,
     "type" : "boolean",
     "exampleValue" : ""
   },
   "userRegisteredDestination" : {
     "title" : "Destination After Successful Self-Registration",
     "description" : "Specifies the behavior when self-registration has successfully completed.",
     "propertyOrder" : 800,
     "required" : true,
     "type" : "string",
     "exampleValue" : ""
   },
   "selfServiceEnabled" : {
     "title" : "Legacy Self-Service REST Endpoint",
     "description" : "Specify whether to enable the legacy self-service endpoint.<p>OpenAM supports
two User Self-Service components: the Legacy User Self-Service, which is based on a Java SDK and is
available in OpenAM versions prior to OpenAM 13, and a common REST-based/XUI-based User Self-Service
available in OpenAM 13 and later.<p>The Legacy User Self-Service will be deprecated in a future
release.",
     "propertyOrder" : 100,
     "required" : true,
     "type" : "boolean",
     "exampleValue" : ""
   },
   "selfRegistrationEnabled" : {
     "title" : "Self-Registration for Users",
     "description" : "If enabled, new users can sign up using a REST API client.",
     "propertyOrder" : 200,
     "required" : true,
     "type" : "boolean",
     "exampleValue" : ""
   },
   "selfRegistrationConfirmationUrl" : {
     "title" : "Self-Registration Confirmation Email URL",
     "description" : "This page handles the HTTP GET request when the user clicks the link sent by
email in the confirmation request.",
     "propertyOrder" : 400,
     "required" : true,
     "type" : "string",
     "exampleValue" : ""
   },
   "forgotPasswordTokenLifetime" : {
     "title" : "Forgot Password Token Lifetime (seconds)",
     "description" : "Maximum life time for the token that allows a user to process a forgotten
password using the REST API.",
     "propertyOrder" : 600,
     "required" : true,
```

```
      "type" : "integer",
      "exampleValue" : ""
    },
    "selfRegistrationTokenLifetime" : {
      "title" : "Self-Registration Token LifeTime (seconds)",
      "description" : "Maximum life time for the token allowing User Self-Registration using the REST
 API.",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "forgotPasswordConfirmationUrl" : {
      "title" : "Forgot Password Confirmation Email URL",
      "description" : "This page handles the HTTP GET request when the user clicks the link sent by
 email in the confirmation request.",
      "propertyOrder" : 700,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "protectedUserAttributes" : {
      "title" : "Protected User Attributes",
      "description" : "A list of user profile attributes. Users modifying any of the attributes in
 this list will be required to enter a password as confirmation before the change is accepted. This
 option applies to XUI deployments only.",
      "propertyOrder" : 900,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    }
  }
}
```


Global Operations

Resource path: `/global-config/services/security`

Resource version: `1.0`

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action LegacyUserSelfService --global --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action LegacyUserSelfService --global --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action LegacyUserSelfService --global --actionName nextdescendents
```

read

Usage:

```
am> read LegacyUserSelfService --global
```

update

Usage:

```
am> update LegacyUserSelfService --global --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "defaults" : {
      "properties" : {
        "confirmationIdHmacKey" : {
          "title" : "Confirmation Id HMAC Signing Key",
          "description" : "256-bit key (base64-encoded) to use for HMAC signing of the legacy self-
service confirmation email links.",
          "propertyOrder" : 1000,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "forgotPasswordEnabled" : {
          "title" : "Forgot Password for Users",
          "description" : "If enabled, users can assign themselves a new password using a REST API
 client.",
          "propertyOrder" : 500,
```

```
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "forgotPasswordConfirmationUrl" : {
          "title" : "Forgot Password Confirmation Email URL",
          "description" : "This page handles the HTTP GET request when the user clicks the link sent
by email in the confirmation request.",
          "propertyOrder" : 700,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "protectedUserAttributes" : {
          "title" : "Protected User Attributes",
          "description" : "A list of user profile attributes. Users modifying any of the attributes in
this list will be required to enter a password as confirmation before the change is accepted. This
option applies to XUI deployments only.",
          "propertyOrder" : 900,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "forgotPasswordTokenLifetime" : {
          "title" : "Forgot Password Token Lifetime (seconds)",
          "description" : "Maximum life time for the token that allows a user to process a forgotten
password using the REST API.",
          "propertyOrder" : 600,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "selfServiceEnabled" : {
          "title" : "Legacy Self-Service REST Endpoint",
          "description" : "Specify whether to enable the legacy self-service endpoint.<p>OpenAM
supports two User Self-Service components: the Legacy User Self-Service, which is based on a Java
SDK and is available in OpenAM versions prior to OpenAM 13, and a common REST-based/XUI-based User
Self-Service available in OpenAM 13 and later.<p>The Legacy User Self-Service will be deprecated in a
future release.",
          "propertyOrder" : 100,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "userRegisteredDestination" : {
          "title" : "Destination After Successful Self-Registration",
          "description" : "Specifies the behavior when self-registration has successfully completed.",
          "propertyOrder" : 800,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "selfRegistrationEnabled" : {
          "title" : "Self-Registration for Users",
          "description" : "If enabled, new users can sign up using a REST API client.",
          "propertyOrder" : 200,
```

```
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "selfRegistrationTokenLifetime" : {
          "title" : "Self-Registration Token LifeTime (seconds)",
          "description" : "Maximum life time for the token allowing User Self-Registration using the
 REST API.",
          "propertyOrder" : 300,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "selfRegistrationConfirmationUrl" : {
          "title" : "Self-Registration Confirmation Email URL",
          "description" : "This page handles the HTTP GET request when the user clicks the link sent
 by email in the confirmation request.",
          "propertyOrder" : 400,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      },
      "type" : "object",
      "title" : "Realm Defaults"
    }
  }
}
```


LinkedInClient

Realm Operations

Resource path: `/realm-config/services/SocialIdentityProviders/linkedInConfig`

Resource version: `1.0`

create

Usage:

```
am> create LinkedInClient --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "tokenEndpoint" : {
      "title" : "Access Token Endpoint URL",
      "description" : "OAuth access token endpoint URL This is the URL endpoint for access token
 retrieval provided by the OAuth Identity Provider.Refer to the RFC 6749 (http://tools.ietf.org/html/
rfc6749#section-3.2), section 3.2.",
      "propertyOrder" : 500,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "clientSecret" : {
      "title" : "Client Secret",
      "description" : "OAuth client_secret parameter <p>For more information on the OAuth client_id
 parameter refer to the RFC 6749 (http://tools.ietf.org/html/rfc6749#section-2.3.1), section 2.3.1.",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "string",
      "format" : "password",
      "exampleValue" : ""
    },
    "authenticationIdKey" : {
      "title" : "Auth ID Key",
      "description" : "Field used to identify a user by the social provider.",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "exampleValue" : "sub"
    },
    "pkceMethod" : {
      "title" : "PKCE Method",
      "description" : "The PKCE transformation method to use when making requests to the authorization
 endpoint.",
      "propertyOrder" : 1100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "basicAuth" : {
      "title" : "Use Basic Auth",
      "description" : "When enabled, the client will use basic auth for authenticating with the social
 auth provider. Enabled by default.",
      "propertyOrder" : 1000,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "redirectURI" : {
      "title" : "Redirect URL",
      "description" : "",
      "propertyOrder" : 700,
      "required" : true,
      "type" : "string",
```

```
      "exampleValue" : ""
    },
    "enabled" : {
      "title" : "Enabled",
      "description" : "",
      "propertyOrder" : 1,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "emailAddressEndpoint" : {
      "title" : "Email Address Endpoint",
      "description" : "The endpoint for retrieving the email address.",
      "propertyOrder" : 1200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "scopeDelimiter" : {
      "title" : "Scope Delimiter",
      "description" : "The delimiter used by an auth server to separate scopes.",
      "propertyOrder" : 800,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "transform" : {
      "title" : "Transform Script",
      "description" : "A script that takes the raw profile object as input and outputs the normalized
profile object.",
      "propertyOrder" : 10000,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "clientId" : {
      "title" : "Client ID",
      "description" : "OAuth client_id parameter<p> For more information on the OAuth client_id
parameter refer to the RFC 6749 (http://tools.ietf.org/html/rfc6749#section-2.3.1), section 2.3.1.",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "uiConfig" : {
      "title" : "UI Config Properties",
      "description" : "Mapping of display properties to be defined and consumed by the UI.",
      "propertyOrder" : 9999,
      "required" : true,
      "patternProperties" : {
        ".*" : {
          "type" : "string"
        }
      },
      "type" : "object",
      "exampleValue" : ""
    },
    "authorizationEndpoint" : {
      "title" : "Authentication Endpoint URL",
```

```
      "description" : "OAuth authentication endpoint URL <p> This is the URL endpoint for OAuth
 authentication provided by the OAuth Identity Provider.",
      "propertyOrder" : 400,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "scopes" : {
      "title" : "OAuth Scopes",
      "description" : "List of user profile properties<p>According to the OAuth 2.0 Authorization
 Framework that the client application requires. The list depends on the permissions that the resource
 owner grants to the client application. Some authorization servers use non-standard separators for
 scopes.",
      "propertyOrder" : 900,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "minItems" : 1,
      "type" : "array",
      "exampleValue" : ""
    },
    "userInfoEndpoint" : {
      "title" : "User Profile Service URL",
      "description" : "User profile information URL <p> This URL endpoint provides user profile
 information and is provided by the OAuth Identity Provider NB This URL should return JSON objects in
 response.",
      "propertyOrder" : 600,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
```

delete

Usage:

```
am> delete LinkedInClient --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action LinkedInClient --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action LinkedInClient --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action LinkedInClient --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query LinkedInClient --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read LinkedInClient --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update LinkedInClient --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "tokenEndpoint" : {
      "title" : "Access Token Endpoint URL",
      "description" : "OAuth access token endpoint URL This is the URL endpoint for access token
 retrieval provided by the OAuth Identity Provider.Refer to the RFC 6749 (http://tools.ietf.org/html/
rfc6749#section-3.2), section 3.2.",
      "propertyOrder" : 500,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "clientSecret" : {
      "title" : "Client Secret",
      "description" : "OAuth client_secret parameter <p>For more information on the OAuth client_id
 parameter refer to the RFC 6749 (http://tools.ietf.org/html/rfc6749#section-2.3.1), section 2.3.1.",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "string",
      "format" : "password",
      "exampleValue" : ""
    },
    "authenticationIdKey" : {
      "title" : "Auth ID Key",
      "description" : "Field used to identify a user by the social provider.",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "exampleValue" : "sub"
    },
    "pkceMethod" : {
      "title" : "PKCE Method",
      "description" : "The PKCE transformation method to use when making requests to the authorization
 endpoint.",
      "propertyOrder" : 1100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "basicAuth" : {
      "title" : "Use Basic Auth",
      "description" : "When enabled, the client will use basic auth for authenticating with the social
 auth provider. Enabled by default.",
      "propertyOrder" : 1000,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "redirectURI" : {
      "title" : "Redirect URL",
```

```
      "description" : "",
      "propertyOrder" : 700,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "enabled" : {
      "title" : "Enabled",
      "description" : "",
      "propertyOrder" : 1,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "emailAddressEndpoint" : {
      "title" : "Email Address Endpoint",
      "description" : "The endpoint for retrieving the email address.",
      "propertyOrder" : 1200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "scopeDelimiter" : {
      "title" : "Scope Delimiter",
      "description" : "The delimiter used by an auth server to separate scopes.",
      "propertyOrder" : 800,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "transform" : {
      "title" : "Transform Script",
      "description" : "A script that takes the raw profile object as input and outputs the normalized
profile object.",
      "propertyOrder" : 10000,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "clientId" : {
      "title" : "Client ID",
      "description" : "OAuth client_id parameter<p> For more information on the OAuth client_id
parameter refer to the RFC 6749 (http://tools.ietf.org/html/rfc6749#section-2.3.1), section 2.3.1.",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "uiConfig" : {
      "title" : "UI Config Properties",
      "description" : "Mapping of display properties to be defined and consumed by the UI.",
      "propertyOrder" : 9999,
      "required" : true,
      "patternProperties" : {
        ".*" : {
          "type" : "string"
        }
      },
      "type" : "object",
```

```
      "exampleValue" : ""
    },
    "authorizationEndpoint" : {
      "title" : "Authentication Endpoint URL",
      "description" : "OAuth authentication endpoint URL <p> This is the URL endpoint for OAuth
 authentication provided by the OAuth Identity Provider.",
      "propertyOrder" : 400,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "scopes" : {
      "title" : "OAuth Scopes",
      "description" : "List of user profile properties<p>According to the OAuth 2.0 Authorization
 Framework that the client application requires. The list depends on the permissions that the resource
 owner grants to the client application. Some authorization servers use non-standard separators for
 scopes.",
      "propertyOrder" : 900,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "minItems" : 1,
      "type" : "array",
      "exampleValue" : ""
    },
    "userInfoEndpoint" : {
      "title" : "User Profile Service URL",
      "description" : "User profile information URL <p> This URL endpoint provides user profile
 information and is provided by the OAuth Identity Provider NB This URL should return JSON objects in
 response.",
      "propertyOrder" : 600,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
```

Logging

Global Operations

Resource path: `/global-config/services/logging`

Resource version: `1.0`

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action Logging --global --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action Logging --global --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action Logging --global --actionName nextdescendents
```

read

Usage:

```
am> read Logging --global
```

update

Usage:

```
am> update Logging --global --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "general" : {
      "type" : "object",
      "title" : "General",
      "propertyOrder" : 0,
      "properties" : {
        "verifyPeriod" : {
          "title" : "Log Verification Frequency",
          "description" : "The frequency (in seconds) that OpenAM verifies security of the log
 files.<br><br>When secure logging is enabled, this is the period that OpenAM will check the integrity
 of the log files.",
          "propertyOrder" : 2000,
```

```
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "security" : {
          "title" : "Secure Logging",
          "description" : "Enable or Disable secure logging.<br><br>Enabling this setting will cause
OpenAM to digitally sign and verify the contents of the log files to help prevent and detect log file
tampering. A certificate must be configured for this functionality to be enabled. ",
          "propertyOrder" : 2200,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "status" : {
          "title" : "Log Status",
          "description" : "Enable the OpenAM logging system.<p><p>OpenAM supports two Audit Logging
Services: the legacy Logging Service, which is based on a Java SDK and is available in OpenAM
versions prior to OpenAM 13.5, and a new common REST-based Audit Logging Service available from
OpenAM 13.5.<p><p>The legacy Logging Service will be deprecated in a future release.",
          "propertyOrder" : 800,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "resolveHostName" : {
          "title" : "Log Record Resolve Host Name",
          "description" : "Enable this to have OpenAM perform a DNS host lookup to populate the host
name field for log records.<br><br><i>Note:</i> Enabling this functionality will increase the load of
the logging system and the OpenAM host must have DNS configured. ",
          "propertyOrder" : 900,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "filesPerKeystore" : {
          "title" : "Number of Files per Archive",
          "description" : "Controls the number of logs files that will be archived by the secure
logging system.",
          "propertyOrder" : 2600,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "type" : {
          "title" : "Logging Type",
          "description" : "Specifies whether to log to a database, Syslog, or to the filing
system.<br><br>If you choose database then be sure to set the connection attributes correctly,
including the JDBC driver to use.",
          "propertyOrder" : 1000,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "fields" : {
          "title" : "Configurable Log Fields",
          "description" : "Controls the fields that are logged by OpenAM.<br><br>This property is the
list of fields that are logged by default. Administrators can choose to limit the information logged
by OpenAM.",
```

```
          "propertyOrder" : 1900,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "buffering" : {
          "title" : "Time Buffering",
          "description" : "Enable or Disable log buffering<br><br>When enabled OpenAM holds all log
records in a memory buffer that it periodically flush to the repository. The period is set in the
<i>Buffer Time</i> property.",
          "propertyOrder" : 3000,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "certificateStore" : {
          "title" : "Logging Certificate Store Location",
          "description" : "The path to the Java keystore containing the logging system
certificate.<br><br>The secure logging system will use the certificate alias of <code>Logger</code>
to locate the certificate in the specified keystore.",
          "propertyOrder" : 2400,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "signingAlgorithm" : {
          "title" : "Secure Logging Signing Algorithm ",
          "description" : "Determines the algorithm used to digitally sign the log records.",
          "propertyOrder" : 2300,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "bufferTime" : {
          "title" : "Buffer Time",
          "description" : "The maximum time (in seconds) OpenAM will hold log records in memory before
flushing to the underlying repository.",
          "propertyOrder" : 2900,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "jdkLoggingLevel" : {
          "title" : "Logging Level",
          "description" : "Control the level of JDK logging within OpenAM. ",
          "propertyOrder" : 3100,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "bufferSize" : {
          "title" : "Buffer Size",
          "description" : "The number of log records held in memory before the log records will be
flushed to the logfile or the database.",
          "propertyOrder" : 2700,
          "required" : true,
```

```
          "type" : "integer",
          "exampleValue" : ""
        },
        "signaturePeriod" : {
          "title" : "Log Signature Time",
          "description" : "The frequency (in seconds) that OpenAM will digitally sign the log
records.<br><br>When secure logging is enabled, this is the period that OpenAM will digitally
signed the contents of the log files. The log signatures form the basis of the log file integrity
checking.",
          "propertyOrder" : 2100,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        }
      }
    },
    "database" : {
      "type" : "object",
      "title" : "Database",
      "propertyOrder" : 2,
      "properties" : {
        "maxRecords" : {
          "title" : "Maximum Number of Records",
          "description" : "The maximum number of records read from the logs via the Logging API",
          "propertyOrder" : 2500,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "databaseFailureMemoryBufferSize" : {
          "title" : "DB Failure Memory Buffer Size",
          "description" : "Max number of log records held in memory if DB logging fails.<br><br>This
is the maximum number of log records that will be held in memory if the database is unavailable.
When the buffer is full, new log records cause the oldest record in the buffer to be cleared. OpenAM
monitoring records the number of log entries cleared when the database was unavailable.<br/><br/>If
the value of this property is less than that of the <i>Buffer Size</i> then the buffer size value
will take precedence. ",
          "propertyOrder" : 2800,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "password" : {
          "title" : "Database User Password",
          "description" : "When logging to a database, set this to the password used to connect to the
database. If this attribute is incorrectly set, OpenAM performance suffers.",
          "propertyOrder" : 1200,
          "required" : true,
          "type" : "string",
          "format" : "password",
          "exampleValue" : ""
        },
        "driver" : {
          "title" : "Database Driver Name",
          "description" : "When logging to a database, set this to the class name of the JDBC driver
used to connect to the database.<br><br>The default is for Oracle. OpenAM also works with the MySQL
database driver.",
          "propertyOrder" : 1300,
          "required" : true,
```

```
          "type" : "string",
          "exampleValue" : ""
        },
        "user" : {
          "title" : "Database User Name",
          "description" : "When logging to a database, set this to the user name used to connect to
 the database. If this attribute is incorrectly set, OpenAM performance suffers.",
          "propertyOrder" : 1100,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "syslog" : {
      "type" : "object",
      "title" : "Syslog",
      "propertyOrder" : 3,
      "properties" : {
        "host" : {
          "title" : "Syslog server host",
          "description" : "The URL or IP address of the syslog server, for example <code>http://
mysyslog.example.com</code>, or <code>localhost</code>.",
          "propertyOrder" : 1400,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "port" : {
          "title" : "Syslog server port",
          "description" : "The port number the syslog server is configured to listen to.",
          "propertyOrder" : 1500,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "facility" : {
          "title" : "Syslog facility",
          "description" : "Syslog uses the facility level to determine the type of program that is
 logging the message.",
          "propertyOrder" : 1700,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "protocol" : {
          "title" : "Syslog transport protocol",
          "description" : "The protocol to use to connect to the syslog server.",
          "propertyOrder" : 1600,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "timeout" : {
          "title" : "Syslog connection timeout",
          "description" : "The amount of time to wait when attempting to connect to the syslog server
 before reporting a failure, in seconds.",
          "propertyOrder" : 1800,
          "required" : true,
```

```
          "type" : "integer",
          "exampleValue" : ""
        }
      }
    },
    "file" : {
      "type" : "object",
      "title" : "File",
      "propertyOrder" : 1,
      "properties" : {
        "numberHistoryFiles" : {
          "title" : "Number of History Files",
          "description" : "Sets the number of history files for each log that OpenAM keeps, including
 time-based histories.<p><p>The previously live file is moved and is included in the history count,
 and a new log is created to serve as the live log file. Any log file in the history count that goes
 over the number specified here will be deleted.<p><p>For time-based logs, a new set of logs will be
 created when OpenAM is started because of the time-based file names that are used.",
          "propertyOrder" : 300,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "rotationEnabled" : {
          "title" : "Log Rotation",
          "description" : "Enable log rotation to cause new log files to be created when configured
 thresholds are reached, such as <i>Maximum Log Size</i> or <i>Logfile Rotation Interval</i>.",
          "propertyOrder" : 100,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "suffix" : {
          "title" : "Logfile Rotation Suffix",
          "description" : "The name of the log files will be suffixed with the supplied
 value.<br><br>This field defines the log file suffix. If no suffix is provided, then the following
 default suffix format will be used: <code>-MM.dd.yy-kk.mm</code>. The suffix allows use of Date
 and Time patterns defined in <a href=\"http://download.oracle.com/javase/6/docs/api/java/text/
SimpleDateFormat.html\"><code>SimpleDateFormat</code></a><p><p><i>Note:</i> This field is only used if
 the time based rotation is enabled.",
          "propertyOrder" : 500,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "maxFileSize" : {
          "title" : "Maximum Log Size",
          "description" : "Maximum size of a log file, in bytes.",
          "propertyOrder" : 200,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "rotationInterval" : {
          "title" : "Logfile Rotation Interval",
          "description" : "The rotation interval (in minutes).<br><br>The rotation interval determines
 the frequency of when the log files will be rotated. If the value is <code>-1</code>, then time based
 rotation is disabled and log file size based rotation is enabled.",
          "propertyOrder" : 600,
          "required" : true,
```

```
          "type" : "integer",
          "exampleValue" : ""
        },
        "prefix" : {
          "title" : "Logfile Rotation Prefix",
          "description" : "The name of the log files will be prefixed with the supplied
 value.<br><br>This field defines the log file prefix. The prefix will be added to the name of all
 logfiles.<br/><br/><i>Note:</i> Only used when time-based log rotation is enabled.",
          "propertyOrder" : 400,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "location" : {
          "title" : "Log File Location",
          "description" : "The path to the location of the log files<br><br>This property controls
 the location of the log files; the value of this property varies on whether File or DB logging is
 in use:<p><ul><li>File: The full pathname to the directory containing the log files.</li><li>DB: The
 JDBC URL to the database used to store the log file database.</li></ul>",
          "propertyOrder" : 700,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    }
  }
}
```

LoginCountDecision

Realm Operations

Resource path: `/realm-config/authentication/authenticationtrees/nodes/LoginCountDecisionNode`

Resource version: `1.0`

create

Usage:

```
am> create LoginCountDecision --realm Realm --id id --body body
```

Parameters:

`--id`

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "identityAttribute" : {
      "title" : "Identity Attribute",
      "description" : "The attribute of the IDM object to use retrieve the object.",
      "propertyOrder" : 300,
      "type" : "string",
      "exampleValue" : ""
    },
    "interval" : {
      "title" : "Interval",
      "description" : "The interval type for which the decision should occur. Valid types are 'every'
 and 'at'.",
      "propertyOrder" : 100,
      "type" : "string",
      "exampleValue" : ""
    },
    "amount" : {
      "title" : "Amount",
      "description" : "The amount (count) of logins for the interval.",
      "propertyOrder" : 200,
      "type" : "integer",
      "exampleValue" : ""
    }
  },
  "required" : [ "identityAttribute", "interval", "amount" ]
}
```

delete

Usage:

```
am> delete LoginCountDecision --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action LoginCountDecision --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action LoginCountDecision --realm Realm --actionName getCreatableTypes
```

listOutcomes

List the available outcomes for the node type.

Usage:

```
am> action LoginCountDecision --realm Realm --body body --actionName listOutcomes
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "title" : "Some configuration of the node. This does not need to be complete against the
 configuration schema."
}
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action LoginCountDecision --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query LoginCountDecision --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read LoginCountDecision --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update LoginCountDecision --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "identityAttribute" : {
      "title" : "Identity Attribute",
      "description" : "The attribute of the IDM object to use retrieve the object.",
      "propertyOrder" : 300,
      "type" : "string",
      "exampleValue" : ""
    },
    "interval" : {
      "title" : "Interval",
      "description" : "The interval type for which the decision should occur. Valid types are 'every'
 and 'at'.",
      "propertyOrder" : 100,
      "type" : "string",
      "exampleValue" : ""
    },
    "amount" : {
      "title" : "Amount",
      "description" : "The amount (count) of logins for the interval.",
      "propertyOrder" : 200,
      "type" : "integer",
      "exampleValue" : ""
    }
  },
  "required" : [ "identityAttribute", "interval", "amount" ]
}
```

MembershipModule

Realm Operations

Resource path: `/realm-config/authentication/modules/membership`

Resource version: `1.0`

create

Usage:

```
am> create MembershipModule --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "defaultUserStatus" : {
      "title" : "User Status After Registration",
      "description" : "Determines if the user account should be automatically active after
 registration completes.",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "authenticationLevel" : {
      "title" : "Authentication Level",
      "description" : "The authentication level associated with this module.<br><br>Each
 authentication module has an authentication level that can be used to indicate the level of security
 associated with the module; 0 is the lowest (and the default).",
      "propertyOrder" : 400,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "minimumPasswordLength" : {
      "title" : "Minimum Password Length",
      "description" : "The minimum length of the user password.<br><br>Setting this value to 0
 disables this functionality.<br/><br/><i>NB </i>This feature is separate from any password policy in
 the underlying data store",
      "propertyOrder" : 100,
```

```
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "defaultUserRoles" : {
      "title" : "Default User Roles",
      "description" : "The role DN's that will be assigned to the user.<br><br><i>NB </i>Roles are
 only supported in Sun Directory Server Enterprise Edition",
      "propertyOrder" : 200,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    }
  }
}
```

delete

Usage:

```
am> delete MembershipModule --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action MembershipModule --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action MembershipModule --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action MembershipModule --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query MembershipModule --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read MembershipModule --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update MembershipModule --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "defaultUserStatus" : {
```

```
      "title" : "User Status After Registration",
      "description" : "Determines if the user account should be automatically active after
 registration completes.",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "authenticationLevel" : {
      "title" : "Authentication Level",
      "description" : "The authentication level associated with this module.<br><br>Each
 authentication module has an authentication level that can be used to indicate the level of security
 associated with the module; 0 is the lowest (and the default).",
      "propertyOrder" : 400,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "minimumPasswordLength" : {
      "title" : "Minimum Password Length",
      "description" : "The minimum length of the user password.<br><br>Setting this value to 0
 disables this functionality.<br/><br/><i>NB </i>This feature is separate from any password policy in
 the underlying data store",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "defaultUserRoles" : {
      "title" : "Default User Roles",
      "description" : "The role DN's that will be assigned to the user.<br><br><i>NB </i>Roles are
 only supported in Sun Directory Server Enterprise Edition",
      "propertyOrder" : 200,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    }
  }
}
```

Global Operations

Resource path: `/global-config/authentication/modules/membership`

Resource version: `1.0`

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action MembershipModule --global --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action MembershipModule --global --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action MembershipModule --global --actionName nextdescendents
```

read

Usage:

```
am> read MembershipModule --global
```

update

Usage:

```
am> update MembershipModule --global --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "defaults" : {
      "properties" : {
        "defaultUserRoles" : {
          "title" : "Default User Roles",
          "description" : "The role DN's that will be assigned to the user.<br><br><i>NB </i>Roles are
 only supported in Sun Directory Server Enterprise Edition",
          "propertyOrder" : 200,
          "required" : true,
          "items" : {
            "type" : "string"
          },
```

```
          "type" : "array",
          "exampleValue" : ""
        },
        "authenticationLevel" : {
          "title" : "Authentication Level",
          "description" : "The authentication level associated with this module.<br><br>Each
 authentication module has an authentication level that can be used to indicate the level of security
 associated with the module; 0 is the lowest (and the default).",
          "propertyOrder" : 400,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "minimumPasswordLength" : {
          "title" : "Minimum Password Length",
          "description" : "The minimum length of the user password.<br><br>Setting this value to 0
 disables this functionality.<br/><br/><i>NB </i>This feature is separate from any password policy in
 the underlying data store",
          "propertyOrder" : 100,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "defaultUserStatus" : {
          "title" : "User Status After Registration",
          "description" : "Determines if the user account should be automatically active after
 registration completes.",
          "propertyOrder" : 300,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      },
      "type" : "object",
      "title" : "Realm Defaults"
    }
  }
}
```

MessageNode

Realm Operations

Resource path: `/realm-config/authentication/authenticationtrees/nodes/MessageNode`

Resource version: `1.0`

create

Usage:

```
am> create MessageNode --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "message" : {
      "title" : "Message",
      "description" : "Localisation overrides - as key fill shortcut for language (first will be used
 as default if not empty or \"Default message\" if empty), value is message for language defined by
 key.",
      "propertyOrder" : 100,
      "patternProperties" : {
        ".*" : {
          "type" : "string"
        }
      },
      "type" : "object",
      "exampleValue" : ""
    },
    "stateField" : {
      "title" : "Shared State Property Name",
      "description" : "",
      "propertyOrder" : 400,
      "type" : "string",
      "exampleValue" : ""
    },
    "messageNo" : {
      "title" : "Negative answer",
      "description" : "Localisation overrides - as key fill shortcut for language (first will be used
 as default if not empty or \"No\" if empty), value is negative answer for language defined by key.",
      "propertyOrder" : 300,
      "patternProperties" : {
        ".*" : {
          "type" : "string"
        }
      },
      "type" : "object",
      "exampleValue" : ""
    },
    "messageYes" : {
      "title" : "Positive answer",
      "description" : "Localisation overrides - as key fill shortcut for language (first will be used
 as default if not empty or \"Yes\" if empty), value is positive answer for language defined by key.",
      "propertyOrder" : 200,
      "patternProperties" : {
        ".*" : {
          "type" : "string"
```

```
        }
      },
      "type" : "object",
      "exampleValue" : ""
    }
  },
  "required" : [ "message", "messageYes", "messageNo" ]
}
```

delete

Usage:

```
am> delete MessageNode --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action MessageNode --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action MessageNode --realm Realm --actionName getCreatableTypes
```

listOutcomes

List the available outcomes for the node type.

Usage:

```
am> action MessageNode --realm Realm --body body --actionName listOutcomes
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "title" : "Some configuration of the node. This does not need to be complete against the
 configuration schema."
}
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action MessageNode --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query MessageNode --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read MessageNode --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update MessageNode --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "message" : {
      "title" : "Message",
      "description" : "Localisation overrides - as key fill shortcut for language (first will be used
 as default if not empty or \"Default message\" if empty), value is message for language defined by
 key.",
      "propertyOrder" : 100,
      "patternProperties" : {
        ".*" : {
          "type" : "string"
        }
      },
      "type" : "object",
      "exampleValue" : ""
    },
    "stateField" : {
      "title" : "Shared State Property Name",
      "description" : "",
      "propertyOrder" : 400,
      "type" : "string",
      "exampleValue" : ""
    },
    "messageNo" : {
      "title" : "Negative answer",
      "description" : "Localisation overrides - as key fill shortcut for language (first will be used
 as default if not empty or \"No\" if empty), value is negative answer for language defined by key.",
      "propertyOrder" : 300,
      "patternProperties" : {
        ".*" : {
          "type" : "string"
        }
      },
      "type" : "object",
      "exampleValue" : ""
    },
    "messageYes" : {
      "title" : "Positive answer",
      "description" : "Localisation overrides - as key fill shortcut for language (first will be used
 as default if not empty or \"Yes\" if empty), value is positive answer for language defined by key.",
      "propertyOrder" : 200,
      "patternProperties" : {
        ".*" : {
          "type" : "string"
        }
      },
      "type" : "object",
      "exampleValue" : ""
    }
  },
```

```
  "required" : [ "message", "messageYes", "messageNo" ]
}
```

Meter

Realm Operations

Resource path: `/realm-config/authentication/authenticationtrees/nodes/MeterNode`

Resource version: `1.0`

create

Usage:

```
am> create Meter --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "metricKey" : {
      "title" : "Metric Key",
      "description" : "Identifier of metric to update when this node is processed.",
      "propertyOrder" : 100,
      "type" : "string",
      "exampleValue" : ""
    }
  },
  "required" : [ "metricKey" ]
}
```

delete

Usage:

```
am> delete Meter --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action Meter --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action Meter --realm Realm --actionName getCreatableTypes
```

listOutcomes

List the available outcomes for the node type.

Usage:

```
am> action Meter --realm Realm --body body --actionName listOutcomes
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "title" : "Some configuration of the node. This does not need to be complete against the
 configuration schema."
}
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action Meter --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query Meter --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read Meter --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update Meter --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "metricKey" : {
      "title" : "Metric Key",
      "description" : "Identifier of metric to update when this node is processed.",
      "propertyOrder" : 100,
      "type" : "string",
      "exampleValue" : ""
    }
  },
  "required" : [ "metricKey" ]
}
```

ModifyAuthLevel

Realm Operations

Resource path: `/realm-config/authentication/authenticationtrees/nodes/ModifyAuthLevelNode`

Resource version: `1.0`

create

Usage:

```
am> create ModifyAuthLevel --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "authLevelIncrement" : {
      "title" : "Value To Add",
      "description" : "Value which is added to the authentication level.Value may be negative to
 decrease the authentication level.",
      "propertyOrder" : 100,
      "type" : "integer",
      "exampleValue" : ""
    }
  },
  "required" : [ "authLevelIncrement" ]
}
```

delete

Usage:

```
am> delete ModifyAuthLevel --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action ModifyAuthLevel --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action ModifyAuthLevel --realm Realm --actionName getCreatableTypes
```

listOutcomes

List the available outcomes for the node type.

Usage:

```
am> action ModifyAuthLevel --realm Realm --body body --actionName listOutcomes
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "title" : "Some configuration of the node. This does not need to be complete against the
 configuration schema."
}
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action ModifyAuthLevel --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query ModifyAuthLevel --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read ModifyAuthLevel --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update ModifyAuthLevel --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "authLevelIncrement" : {
      "title" : "Value To Add",
      "description" : "Value which is added to the authentication level.Value may be negative to
 decrease the authentication level.",
      "propertyOrder" : 100,
      "type" : "integer",
      "exampleValue" : ""
    }
  },
  "required" : [ "authLevelIncrement" ]
}
```

Monitoring

Global Operations

Resource path: `/global-config/services/monitoring`

Resource version: `1.0`

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action Monitoring --global --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action Monitoring --global --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action Monitoring --global --actionName nextdescendents
```

read

Usage:

```
am> read Monitoring --global
```

update

Usage:

```
am> update Monitoring --global --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "snmpEnabled" : {
      "title" : "Monitoring SNMP interface status",
      "description" : "Enable / Disable the SNMP access to the monitoring system",
      "propertyOrder" : 800,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "policyHistoryWindowSize" : {
      "title" : "Policy evaluation monitoring history size",
      "description" : "Size of the window of most recent policy evaluations to record to expose via
 monitoring system. Valid range is 100 - 1000000.",
      "propertyOrder" : 900,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "enabled" : {
      "title" : "Monitoring Status",
      "description" : "Enable / Disable the monitoring system",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "authfilePath" : {
      "title" : "Monitoring HTTP interface authentication file path",
      "description" : "Path to the monitoring system authentication file<br><br>The
 <code>openam_mon_auth</code> file contains the username and password of the account used to
 protect the monitoring interfaces. The default username is <code>demo</code> with a password of
 <code>changeit</code>. Use the <code>ampassword</code> command to encrypt a new password.",
      "propertyOrder" : 400,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "rmiEnabled" : {
      "title" : "Monitoring RMI interface status",
      "description" : "Enable / Disable the JMX access to the monitoring system",
      "propertyOrder" : 600,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "httpEnabled" : {
      "title" : "Monitoring HTTP interface status",
      "description" : "Enable / Disable the HTTP access to the monitoring system ",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
```

```
    "sessionHistoryWindowSize" : {
      "title" : "Session monitoring history size",
      "description" : "Size of the window of most recent session operations to record to expose via
 monitoring system. Valid range is 100 - 1000000.",
      "propertyOrder" : 1000,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "snmpPort" : {
      "title" : "Monitoring SNMP Port",
      "description" : "Port number for the SNMP monitoring interface",
      "propertyOrder" : 700,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "httpPort" : {
      "title" : "Monitoring HTTP Port",
      "description" : "Port number for the HTTP monitoring interface",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "rmiPort" : {
      "title" : "Monitoring RMI Port",
      "description" : "Port number for the JMX monitoring interface",
      "propertyOrder" : 500,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    }
  }
}
```

MsisdnModule

Realm Operations

Resource path: `/realm-config/authentication/modules/msisdn`

Resource version: `1.0`

create

Usage:

```
am> create MsisdnModule --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "userProfileMsisdnAttribute" : {
      "title" : "Attribute To Use To Search LDAP",
      "description" : "The name of the attribute searched in the user profiles for the MSISDN number",
      "propertyOrder" : 500,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "returnUserDN" : {
      "title" : "Return User DN to DataStore",
      "description" : "Controls whether the DN or the username is returned as the authentication
 principal.",
      "propertyOrder" : 1100,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "trustedGatewayIPAddresses" : {
      "title" : "Trusted Gateway IP Address",
      "description" : "The list of IP address that are trusted to send MSISDN authentication
 requests.<br><br>The client IP address of the authentication request is checked against this list, if
 the client IP is not listed then the authentication module will fail.<br/><br/><i>NB </i>If the list
 is empty then all hosts will be trusted.",
      "propertyOrder" : 100,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "msisdnParameterNames" : {
      "title" : "MSISDN Number Search Parameter Name",
      "description" : "Name of the HTTP cookie, header or query parameter containing the MSISDN
 number<br><br>The MSISDN authentication module will check the incoming HTTP cookie, header or
 query parameter of the request for the MSISDN number. The order of checking is as follows:<br/><br/
><ol><li>Cookie</li><li>Header</li><li>Query</li></ol><br/><br/><i>NB </i>The <i>MSISDN Header Search
 Attribute</i> controls what elements of the request is searched",
      "propertyOrder" : 200,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "authenticationLevel" : {
      "title" : "Authentication Level",
```

```
      "description" : "The authentication level associated with this module.<br><br>Each
 authentication module has an authentication level that can be used to indicate the level of security
 associated with the module; 0 is the lowest (and the default).",
      "propertyOrder" : 1200,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "ldapSslEnabled" : {
      "title" : "SSL/TLS for LDAP Access",
      "description" : "",
      "propertyOrder" : 800,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "msisdnRequestSearchLocations" : {
      "title" : "MSISDN Header Search Attribute",
      "description" : "Controls the elements that are searched by the authentication module ",
      "propertyOrder" : 900,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "ldapUserBindDN" : {
      "title" : "LDAP Server Authentication User ",
      "description" : "DN of the user used by the module to authenticate to the LDAP server<br><br>The
 MSISDN module authenticates to the LDAP server in order to search for a matching number. The DN
 entered here represents the account used for said authentication and must have read/search access to
 the LDAP server.",
      "propertyOrder" : 600,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "baseSearchDN" : {
      "title" : "LDAP Start Search DN",
      "description" : "The start point in the LDAP server for the MSISDN search<br><br>When entering
 multiple entries, each entry must be prefixed with a local server name. Multiple entries allow
 different search Base DNs depending on the OpenAM server in use. The format is:<br/><br/><code>local
 server name | base dn</code><br/><br/>The local server name is the full name of the server from the
 list of servers and sites.",
      "propertyOrder" : 400,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "ldapProviderUrl" : {
      "title" : "LDAP Server and Port ",
      "description" : "Use this list to set the LDAP server used to search for the MSISDN number.
 <br><br>The MSISDN authentication module will use this list as the server that is searched for a
 matching MSISDN number. A single entry must be in the format:<br/><br/><code>ldap_server:port</
code><br/><br/>Multiple entries allow associations between OpenAM servers and a LDAP server. The
```

```
 format is:<br/><br/><code>local server name | server:port</code><br/><br/>The local server name is
 the full name of the server from the list of servers and sites.",
      "propertyOrder" : 300,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "ldapUserBindPassword" : {
      "title" : "LDAP Server Authentication Password",
      "description" : "The password for the authentication user",
      "propertyOrder" : 700,
      "required" : true,
      "type" : "string",
      "format" : "password",
      "exampleValue" : ""
    },
    "msisdnUserNamingAttribute" : {
      "title" : "LDAP Attribute Used to Retrieve User Profile",
      "description" : "The name of the attribute returned from the user profile matched against the
 supplied MSISDN number",
      "propertyOrder" : 1000,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
```

delete

Usage:

```
am> delete MsisdnModule --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action MsisdnModule --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action MsisdnModule --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action MsisdnModule --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query MsisdnModule --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read MsisdnModule --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update MsisdnModule --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "userProfileMsisdnAttribute" : {
      "title" : "Attribute To Use To Search LDAP",
      "description" : "The name of the attribute searched in the user profiles for the MSISDN number",
      "propertyOrder" : 500,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "returnUserDN" : {
      "title" : "Return User DN to DataStore",
      "description" : "Controls whether the DN or the username is returned as the authentication
 principal.",
      "propertyOrder" : 1100,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "trustedGatewayIPAddresses" : {
      "title" : "Trusted Gateway IP Address",
      "description" : "The list of IP address that are trusted to send MSISDN authentication
 requests.<br><br>The client IP address of the authentication request is checked against this list, if
 the client IP is not listed then the authentication module will fail.<br/><br/><i>NB </i>If the list
 is empty then all hosts will be trusted.",
      "propertyOrder" : 100,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "msisdnParameterNames" : {
      "title" : "MSISDN Number Search Parameter Name",
      "description" : "Name of the HTTP cookie, header or query parameter containing the MSISDN
 number<br><br>The MSISDN authentication module will check the incoming HTTP cookie, header or
 query parameter of the request for the MSISDN number. The order of checking is as follows:<br/><br/
><ol><li>Cookie</li><li>Header</li><li>Query</li></ol><br/><br/><i>NB </i>The <i>MSISDN Header Search
 Attribute</i> controls what elements of the request is searched",
      "propertyOrder" : 200,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "authenticationLevel" : {
      "title" : "Authentication Level",
```

```
      "description" : "The authentication level associated with this module.<br><br>Each
 authentication module has an authentication level that can be used to indicate the level of security
 associated with the module; 0 is the lowest (and the default).",
      "propertyOrder" : 1200,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "ldapSslEnabled" : {
      "title" : "SSL/TLS for LDAP Access",
      "description" : "",
      "propertyOrder" : 800,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "msisdnRequestSearchLocations" : {
      "title" : "MSISDN Header Search Attribute",
      "description" : "Controls the elements that are searched by the authentication module ",
      "propertyOrder" : 900,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "ldapUserBindDN" : {
      "title" : "LDAP Server Authentication User ",
      "description" : "DN of the user used by the module to authenticate to the LDAP server<br><br>The
 MSISDN module authenticates to the LDAP server in order to search for a matching number. The DN
 entered here represents the account used for said authentication and must have read/search access to
 the LDAP server.",
      "propertyOrder" : 600,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "baseSearchDN" : {
      "title" : "LDAP Start Search DN",
      "description" : "The start point in the LDAP server for the MSISDN search<br><br>When entering
 multiple entries, each entry must be prefixed with a local server name. Multiple entries allow
 different search Base DNs depending on the OpenAM server in use. The format is:<br/><br/><code>local
 server name | base dn</code><br/><br/>The local server name is the full name of the server from the
 list of servers and sites.",
      "propertyOrder" : 400,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "ldapProviderUrl" : {
      "title" : "LDAP Server and Port ",
      "description" : "Use this list to set the LDAP server used to search for the MSISDN number.
 <br><br>The MSISDN authentication module will use this list as the server that is searched for a
 matching MSISDN number. A single entry must be in the format:<br/><br/><code>ldap_server:port</
code><br/><br/>Multiple entries allow associations between OpenAM servers and a LDAP server. The
```

```
 format is:<br/><br/><code>local server name | server:port</code><br/><br/>The local server name is
 the full name of the server from the list of servers and sites.",
      "propertyOrder" : 300,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "ldapUserBindPassword" : {
      "title" : "LDAP Server Authentication Password",
      "description" : "The password for the authentication user",
      "propertyOrder" : 700,
      "required" : true,
      "type" : "string",
      "format" : "password",
      "exampleValue" : ""
    },
    "msisdnUserNamingAttribute" : {
      "title" : "LDAP Attribute Used to Retrieve User Profile",
      "description" : "The name of the attribute returned from the user profile matched against the
 supplied MSISDN number",
      "propertyOrder" : 1000,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
```

Global Operations

Resource path: `/global-config/authentication/modules/msisdn`

Resource version: `1.0`

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action MsisdnModule --global --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action MsisdnModule --global --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action MsisdnModule --global --actionName nextdescendents
```

read

Usage:

```
am> read MsisdnModule --global
```

update

Usage:

```
am> update MsisdnModule --global --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "defaults" : {
      "properties" : {
        "ldapUserBindDN" : {
          "title" : "LDAP Server Authentication User ",
          "description" : "DN of the user used by the module to authenticate to the LDAP
 server<br><br>The MSISDN module authenticates to the LDAP server in order to search for a matching
 number. The DN entered here represents the account used for said authentication and must have read/
search access to the LDAP server.",
          "propertyOrder" : 600,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "ldapSslEnabled" : {
          "title" : "SSL/TLS for LDAP Access",
          "description" : "",
          "propertyOrder" : 800,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "ldapProviderUrl" : {
          "title" : "LDAP Server and Port ",
          "description" : "Use this list to set the LDAP server used to search for the MSISDN number.
 <br><br>The MSISDN authentication module will use this list as the server that is searched for a
```

```
 matching MSISDN number. A single entry must be in the format:<br/><br/><code>ldap_server:port</
code><br/><br/>Multiple entries allow associations between OpenAM servers and a LDAP server. The
 format is:<br/><br/><code>local server name | server:port</code><br/><br/>The local server name is
 the full name of the server from the list of servers and sites.",
          "propertyOrder" : 300,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "msisdnParameterNames" : {
          "title" : "MSISDN Number Search Parameter Name",
          "description" : "Name of the HTTP cookie, header or query parameter containing the MSISDN
 number<br><br>The MSISDN authentication module will check the incoming HTTP cookie, header or
 query parameter of the request for the MSISDN number. The order of checking is as follows:<br/><br/
><ol><li>Cookie</li><li>Header</li><li>Query</li></ol><br/><br/><i>NB </i>The <i>MSISDN Header Search
 Attribute</i> controls what elements of the request is searched",
          "propertyOrder" : 200,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "ldapUserBindPassword" : {
          "title" : "LDAP Server Authentication Password",
          "description" : "The password for the authentication user",
          "propertyOrder" : 700,
          "required" : true,
          "type" : "string",
          "format" : "password",
          "exampleValue" : ""
        },
        "trustedGatewayIPAddresses" : {
          "title" : "Trusted Gateway IP Address",
          "description" : "The list of IP address that are trusted to send MSISDN authentication
 requests.<br><br>The client IP address of the authentication request is checked against this list, if
 the client IP is not listed then the authentication module will fail.<br/><br/><i>NB </i>If the list
 is empty then all hosts will be trusted.",
          "propertyOrder" : 100,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "returnUserDN" : {
          "title" : "Return User DN to DataStore",
          "description" : "Controls whether the DN or the username is returned as the authentication
 principal.",
          "propertyOrder" : 1100,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
```

```
        "authenticationLevel" : {
          "title" : "Authentication Level",
          "description" : "The authentication level associated with this module.<br><br>Each
 authentication module has an authentication level that can be used to indicate the level of security
 associated with the module; 0 is the lowest (and the default).",
          "propertyOrder" : 1200,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "baseSearchDN" : {
          "title" : "LDAP Start Search DN",
          "description" : "The start point in the LDAP server for the MSISDN search<br><br>When
 entering multiple entries, each entry must be prefixed with a local server name. Multiple entries
 allow different search Base DNs depending on the OpenAM server in use. The format is:<br/><br/
><code>local server name | base dn</code><br/><br/>The local server name is the full name of the
 server from the list of servers and sites.",
          "propertyOrder" : 400,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "msisdnUserNamingAttribute" : {
          "title" : "LDAP Attribute Used to Retrieve User Profile",
          "description" : "The name of the attribute returned from the user profile matched against
 the supplied MSISDN number",
          "propertyOrder" : 1000,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "msisdnRequestSearchLocations" : {
          "title" : "MSISDN Header Search Attribute",
          "description" : "Controls the elements that are searched by the authentication module ",
          "propertyOrder" : 900,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "userProfileMsisdnAttribute" : {
          "title" : "Attribute To Use To Search LDAP",
          "description" : "The name of the attribute searched in the user profiles for the MSISDN
 number",
          "propertyOrder" : 500,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      },
      "type" : "object",
      "title" : "Realm Defaults"
    }
  }
```

```
}
```

MultiFederationProtocol

Global Operations

Resource path: `/global-config/services/federation/multi`

Resource version: `1.0`

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action MultiFederationProtocol --global --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action MultiFederationProtocol --global --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action MultiFederationProtocol --global --actionName nextdescendents
```

read

Usage:

```
am> read MultiFederationProtocol --global
```

update

Usage:

```
am> update MultiFederationProtocol --global --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "singleLogoutHandlerList" : {
      "title" : "Single Logout Handler List",
      "description" : "List of Logout handlers for each supported federation protocol<br><br>The
 multi-federation protocol engine supports Single Logout. Each federation protocol
 requires a different single logout handler. Logout handler must implement the
 <code>com.sun.identity.multiprotocol.SingleLogoutHandler</code> interface.",
      "propertyOrder" : 100,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    }
  }
}
```

Naming

Global Operations

Resource path: `/global-config/services/naming`

Resource version: `1.0`

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action Naming --global --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action Naming --global --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action Naming --global --actionName nextdescendents
```

read

Usage:

```
am> read Naming --global
```

update

Usage:

```
am> update Naming --global --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "federationConfig" : {
      "type" : "object",
      "title" : "Federation Configuration",
      "propertyOrder" : 1,
      "properties" : {
        "samlSoapReceiverUrl" : {
          "title" : "SAML SOAP Service URL",
          "description" : "Specifies the SAML v1 SOAP service endpoint.",
          "propertyOrder" : 700,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "samlPostServletUrl" : {
          "title" : "SAML Web Profile/POST Service URL",
          "description" : "Specifies the SAML v1 Web Profile endpoint.",
          "propertyOrder" : 800,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "samlAwareServletUrl" : {
          "title" : "SAML Web Profile/Artifact Service URL",
          "description" : "Specifies the SAML v1 endpoint.",
          "propertyOrder" : 600,
```

```
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "samlAssertionManagerUrl" : {
          "title" : "SAML Assertion Manager Service URL",
          "description" : "Specifies the SAML v1 assertion service endpoint.",
          "propertyOrder" : 900,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "jaxrpcUrl" : {
          "title" : "JAXRPC Endpoint URL",
          "description" : "Specifies the JAXRPC endpoint URL used by the remote IDM/SMS APIs.",
          "propertyOrder" : 1200,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "generalConfig" : {
      "type" : "object",
      "title" : "General Configuration",
      "propertyOrder" : 0,
      "properties" : {
        "profileUrl" : {
          "title" : "Profile Service URL",
          "description" : "Specifies the endpoint used by the profile service.<p><p>This attribute is
deprecated.",
          "propertyOrder" : 100,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "loggingUrl" : {
          "title" : "Logging Service URL",
          "description" : "Specifies the endpoint used by the logging service.",
          "propertyOrder" : 300,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "authUrl" : {
          "title" : "Authentication Service URL",
          "description" : "Specifies the endpoint used by the authentication service.",
          "propertyOrder" : 500,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "sessionUrl" : {
          "title" : "Session Service URL",
          "description" : "Specifies the endpoint used by the session service.",
          "propertyOrder" : 200,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
```

```
        },
        "policyUrl" : {
          "title" : "Policy Service URL",
          "description" : "Specifies the endpoint used by the policy service.",
          "propertyOrder" : 400,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "endpointConfig" : {
      "type" : "object",
      "title" : "Endpoint Configuration",
      "propertyOrder" : 2,
      "properties" : {
        "stsMexUrl" : {
          "title" : "Security Token Service MEX Endpoint URL",
          "description" : "Specifies the STS MEX endpoint.",
          "propertyOrder" : 1600,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "idsvcsRestUrl" : {
          "title" : "Identity REST Services Endpoint URL",
          "description" : "Specifies the endpoint for the Identity REST services.",
          "propertyOrder" : 1400,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "stsUrl" : {
          "title" : "Security Token Service Endpoint URL",
          "description" : "Specifies the STS endpoint.",
          "propertyOrder" : 1500,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "jaxwsUrl" : {
          "title" : "Identity Web Services Endpoint URL",
          "description" : "Specifies the endpoint for the Identity WSDL services.",
          "propertyOrder" : 1300,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    }
  }
}
```

OAuth20

Realm Operations

Resource path: `/realm-config/authentication/authenticationtrees/nodes/SocialNode`

Resource version: `1.0`

create

Usage:

```
am> create OAuth20 --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "tokenEndpoint" : {
      "title" : "Access Token Endpoint URL",
      "description" : "OAuth access token endpoint URL This is the URL endpoint for access token
 retrieval provided by the OAuth Identity Provider.Refer to the RFC 6749 (http://tools.ietf.org/html/
rfc6749#section-3.2), section 3.2.",
      "propertyOrder" : 400,
      "type" : "string",
      "exampleValue" : ""
    },
    "saveUserAttributesToSession" : {
      "title" : "Save Attributes in the Session",
      "description" : "If this option is enabled, the attributes configured in the attribute mapper
 will be saved into the OpenAM session.",
      "propertyOrder" : 1700,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "cfgAccountMapperConfiguration" : {
      "title" : "Account Mapper Configuration",
      "description" : "Mapping of OAuth account to local OpenAM account Attribute configuration that
 will be used to map the account of the user authenticated in the OAuth 2.0 Provider to the local data
 store in the OpenAM. Example: <code>OAuth2.0_attribute=local_attribute</code>",
      "propertyOrder" : 1500,
      "patternProperties" : {
        ".*" : {
          "type" : "string"
```

```
       }
     },
     "type" : "object",
     "exampleValue" : ""
   },
   "provider" : {
     "title" : "Social Provider",
     "description" : "Social Provider for which this module is being setup.",
     "propertyOrder" : 900,
     "type" : "string",
     "exampleValue" : ""
   },
   "issuer" : {
     "title" : "Token Issuer",
     "description" : "Required when the 'openid' scope is included. Value must match the iss field
in issued ID Token e.g. accounts.google.com The issuer value MUST be provided when OAuth 2.0 Mix-Up
Mitigation is enabled.",
     "propertyOrder" : 1900,
     "type" : "string",
     "exampleValue" : ""
   },
   "clientId" : {
     "title" : "Client ID",
     "description" : "OAuth client_id parameter<p> For more information on the OAuth client_id
parameter refer to the RFC 6749 (http://tools.ietf.org/html/rfc6749#section-2.3.1), section 2.3.1.",
     "propertyOrder" : 100,
     "type" : "string",
     "exampleValue" : ""
   },
   "scopeString" : {
     "title" : "OAuth Scope",
     "description" : "List of user profile properties<p>According to the OAuth 2.0 Authorization
Framework, scope is a space-separated list of user profile attributes that the client application
requires. The list depends on the permissions that the resource owner grants to the client
application. Some authorization servers use non-standard separators for scopes.",
     "propertyOrder" : 600,
     "type" : "string",
     "exampleValue" : ""
   },
   "authenticationIdKey" : {
     "title" : "Auth ID Key",
     "description" : "",
     "propertyOrder" : 1000,
     "type" : "string",
     "exampleValue" : ""
   },
   "cfgAccountMapperClass" : {
     "title" : "Account Mapper",
     "description" : "Name of the class implementing the attribute mapping for the
account search. This class is used by the module to map from the account information
received from the OAuth Identity Provider into OpenAM. The class must implement the
<code>org.forgerock.openam.authentication.modules.common.mapping.AttributeMapper</code> interface.
Provided implementations are:
<code>org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper
org.forgerock.openam.authentication.modules.oidc.JwtAttributeMapper</code>(can only be used when
using the openid scope) String constructor parameters can be provided by appending | separated
values.",
     "propertyOrder" : 1300,
     "type" : "string",
```

```
      "exampleValue" : ""
    },
    "cfgAttributeMappingClasses" : {
      "title" : "Attribute Mapper",
      "description" : "Name of the class that implements the attribute
 mapping This class maps the OAuth properties into OpenAM properties. A custom
 attribute mapper can be provided. A custom attribute mapper must implement the
 org.forgerock.openam.authentication.modules.common.mapping.AttributeMapper interface. Provided
 implementations are: org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper
 org.forgerock.openam.authentication.modules.oidc.JwtAttributeMapper (can only be used when using the
 openid scope)",
      "propertyOrder" : 1400,
      "items" : {
        "type" : "string"
      },
      "minItems" : 1,
      "type" : "array",
      "exampleValue" : ""
    },
    "redirectURI" : {
      "title" : "Redirect URL",
      "description" : "",
      "propertyOrder" : 800,
      "type" : "string",
      "exampleValue" : ""
    },
    "cfgMixUpMitigation" : {
      "title" : "OAuth 2.0 Mix-Up Mitigation Enabled",
      "description" : "Enables OAuth 2.0 mix-up mitigation The authorization server must support
 the OAuth 2.0 Mix-Up Mitigation draft (https://tools.ietf.org/html/draft-ietf-oauth-mix-up-
mitigation-01#section-3.1), otherwise OpenAM will fail to validate responses from the authorization
 server. If only the OAuth 2.0 protocol is utilized, make sure that the accepted issuer value is set
 in the \"Token Issuer\" setting.",
      "propertyOrder" : 1800,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "userInfoEndpoint" : {
      "title" : "User Profile Service URL",
      "description" : "User profile information URL <p> This URL endpoint provides user profile
 information and is provided by the OAuth Identity Provider NB This URL should return JSON objects in
 response.",
      "propertyOrder" : 500,
      "type" : "string",
      "exampleValue" : ""
    },
    "cfgAttributeMappingConfiguration" : {
      "title" : "Attribute Mapper Configuration",
      "description" : "Mapping of OAuth attributes to local OpenAM attributes Attribute configuration
 that will be used to map the user info obtained from the OAuth 2.0 Provider to the local user data
 store in the OpenAM. Example: OAuth2.0_attribute=local_attribute",
      "propertyOrder" : 1600,
      "patternProperties" : {
        ".*" : {
          "type" : "string"
        }
      },
      "type" : "object",
      "exampleValue" : ""
```

```
    },
    "scopeDelimiter" : {
      "title" : "Scope Delimiter",
      "description" : "Delimiter used to separate scope values. Default value is space.",
      "propertyOrder" : 700,
      "type" : "string",
      "exampleValue" : ""
    },
    "authorizeEndpoint" : {
      "title" : "Authentication Endpoint URL",
      "description" : "OAuth authentication endpoint URL <p> This is the URL endpoint for OAuth
 authentication provided by the OAuth Identity Provider.",
      "propertyOrder" : 300,
      "type" : "string",
      "exampleValue" : ""
    },
    "basicAuth" : {
      "title" : "Use Basic Auth",
      "description" : "When enabled, the client will use basic auth for authenticating with the social
 auth provider. Enabled by default.",
      "propertyOrder" : 1100,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "cfgAccountProviderClass" : {
      "title" : "Account Provider",
      "description" : "Name of the class implementing the account provider. This class is
 used by the module to find the account from the attributes mapped by the Account Mapper
 <code>org.forgerock.openam.authentication.modules.common.mapping.AccountProvider</code> interface.
 String constructor parameters can be provided by appending | separated values.",
      "propertyOrder" : 1200,
      "type" : "string",
      "exampleValue" : ""
    },
    "clientSecret" : {
      "title" : "Client Secret",
      "description" : "OAuth client_secret parameter <p>For more information on the OAuth client_id
 parameter refer to the RFC 6749 (http://tools.ietf.org/html/rfc6749#section-2.3.1), section 2.3.1.",
      "propertyOrder" : 200,
      "type" : "string",
      "format" : "password",
      "exampleValue" : ""
    }
  },
  "required" : [ "scopeString", "cfgAttributeMappingClasses", "cfgMixUpMitigation",
 "cfgAttributeMappingConfiguration", "scopeDelimiter", "issuer", "userInfoEndpoint", "redirectURI",
 "authenticationIdKey", "cfgAccountMapperConfiguration", "provider", "saveUserAttributesToSession",
 "tokenEndpoint", "authorizeEndpoint", "basicAuth", "clientSecret", "cfgAccountProviderClass",
 "clientId", "cfgAccountMapperClass" ]
}
```

delete

Usage:

```
am> delete OAuth20 --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action OAuth20 --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action OAuth20 --realm Realm --actionName getCreatableTypes
```

listOutcomes

List the available outcomes for the node type.

Usage:

```
am> action OAuth20 --realm Realm --body body --actionName listOutcomes
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "title" : "Some configuration of the node. This does not need to be complete against the
 configuration schema."
}
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action OAuth20 --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query OAuth20 --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read OAuth20 --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update OAuth20 --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "tokenEndpoint" : {
      "title" : "Access Token Endpoint URL",
      "description" : "OAuth access token endpoint URL This is the URL endpoint for access token
 retrieval provided by the OAuth Identity Provider.Refer to the RFC 6749 (http://tools.ietf.org/html/
rfc6749#section-3.2), section 3.2.",
      "propertyOrder" : 400,
      "type" : "string",
      "exampleValue" : ""
    },
```

```
   "saveUserAttributesToSession" : {
     "title" : "Save Attributes in the Session",
     "description" : "If this option is enabled, the attributes configured in the attribute mapper
will be saved into the OpenAM session.",
     "propertyOrder" : 1700,
     "type" : "boolean",
     "exampleValue" : ""
   },
   "cfgAccountMapperConfiguration" : {
     "title" : "Account Mapper Configuration",
     "description" : "Mapping of OAuth account to local OpenAM account Attribute configuration that
will be used to map the account of the user authenticated in the OAuth 2.0 Provider to the local data
store in the OpenAM. Example: <code>OAuth2.0_attribute=local_attribute</code>",
     "propertyOrder" : 1500,
     "patternProperties" : {
       ".*" : {
         "type" : "string"
       }
     },
     "type" : "object",
     "exampleValue" : ""
   },
   "provider" : {
     "title" : "Social Provider",
     "description" : "Social Provider for which this module is being setup.",
     "propertyOrder" : 900,
     "type" : "string",
     "exampleValue" : ""
   },
   "issuer" : {
     "title" : "Token Issuer",
     "description" : "Required when the 'openid' scope is included. Value must match the iss field
in issued ID Token e.g. accounts.google.com The issuer value MUST be provided when OAuth 2.0 Mix-Up
Mitigation is enabled.",
     "propertyOrder" : 1900,
     "type" : "string",
     "exampleValue" : ""
   },
   "clientId" : {
     "title" : "Client ID",
     "description" : "OAuth client_id parameter<p> For more information on the OAuth client_id
parameter refer to the RFC 6749 (http://tools.ietf.org/html/rfc6749#section-2.3.1), section 2.3.1.",
     "propertyOrder" : 100,
     "type" : "string",
     "exampleValue" : ""
   },
   "scopeString" : {
     "title" : "OAuth Scope",
     "description" : "List of user profile properties<p>According to the OAuth 2.0 Authorization
Framework, scope is a space-separated list of user profile attributes that the client application
requires. The list depends on the permissions that the resource owner grants to the client
application. Some authorization servers use non-standard separators for scopes.",
     "propertyOrder" : 600,
     "type" : "string",
     "exampleValue" : ""
   },
   "authenticationIdKey" : {
     "title" : "Auth ID Key",
     "description" : "",
```

```
      "propertyOrder" : 1000,
      "type" : "string",
      "exampleValue" : ""
    },
    "cfgAccountMapperClass" : {
      "title" : "Account Mapper",
      "description" : "Name of the class implementing the attribute mapping for the
 account search. This class is used by the module to map from the account information
 received from the OAuth Identity Provider into OpenAM. The class must implement the
 <code>org.forgerock.openam.authentication.modules.common.mapping.AttributeMapper</code> interface.
 Provided implementations are:
 <code>org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper
 org.forgerock.openam.authentication.modules.oidc.JwtAttributeMapper</code>(can only be used when
 using the openid scope) String constructor parameters can be provided by appending | separated
 values.",
      "propertyOrder" : 1300,
      "type" : "string",
      "exampleValue" : ""
    },
    "cfgAttributeMappingClasses" : {
      "title" : "Attribute Mapper",
      "description" : "Name of the class that implements the attribute
 mapping This class maps the OAuth properties into OpenAM properties. A custom
 attribute mapper can be provided. A custom attribute mapper must implement the
 org.forgerock.openam.authentication.modules.common.mapping.AttributeMapper interface. Provided
 implementations are: org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper
 org.forgerock.openam.authentication.modules.oidc.JwtAttributeMapper (can only be used when using the
 openid scope)",
      "propertyOrder" : 1400,
      "items" : {
        "type" : "string"
      },
      "minItems" : 1,
      "type" : "array",
      "exampleValue" : ""
    },
    "redirectURI" : {
      "title" : "Redirect URL",
      "description" : "",
      "propertyOrder" : 800,
      "type" : "string",
      "exampleValue" : ""
    },
    "cfgMixUpMitigation" : {
      "title" : "OAuth 2.0 Mix-Up Mitigation Enabled",
      "description" : "Enables OAuth 2.0 mix-up mitigation The authorization server must support
 the OAuth 2.0 Mix-Up Mitigation draft (https://tools.ietf.org/html/draft-ietf-oauth-mix-up-
mitigation-01#section-3.1), otherwise OpenAM will fail to validate responses from the authorization
 server. If only the OAuth 2.0 protocol is utilized, make sure that the accepted issuer value is set
 in the \"Token Issuer\" setting.",
      "propertyOrder" : 1800,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "userInfoEndpoint" : {
      "title" : "User Profile Service URL",
      "description" : "User profile information URL <p> This URL endpoint provides user profile
 information and is provided by the OAuth Identity Provider NB This URL should return JSON objects in
 response.",
```

```
     "propertyOrder" : 500,
     "type" : "string",
     "exampleValue" : ""
   },
   "cfgAttributeMappingConfiguration" : {
     "title" : "Attribute Mapper Configuration",
     "description" : "Mapping of OAuth attributes to local OpenAM attributes Attribute configuration
that will be used to map the user info obtained from the OAuth 2.0 Provider to the local user data
store in the OpenAM. Example: OAuth2.0_attribute=local_attribute",
     "propertyOrder" : 1600,
     "patternProperties" : {
       ".*" : {
         "type" : "string"
       }
     },
     "type" : "object",
     "exampleValue" : ""
   },
   "scopeDelimiter" : {
     "title" : "Scope Delimiter",
     "description" : "Delimiter used to separate scope values. Default value is space.",
     "propertyOrder" : 700,
     "type" : "string",
     "exampleValue" : ""
   },
   "authorizeEndpoint" : {
     "title" : "Authentication Endpoint URL",
     "description" : "OAuth authentication endpoint URL <p> This is the URL endpoint for OAuth
authentication provided by the OAuth Identity Provider.",
     "propertyOrder" : 300,
     "type" : "string",
     "exampleValue" : ""
   },
   "basicAuth" : {
     "title" : "Use Basic Auth",
     "description" : "When enabled, the client will use basic auth for authenticating with the social
auth provider. Enabled by default.",
     "propertyOrder" : 1100,
     "type" : "boolean",
     "exampleValue" : ""
   },
   "cfgAccountProviderClass" : {
     "title" : "Account Provider",
     "description" : "Name of the class implementing the account provider. This class is
used by the module to find the account from the attributes mapped by the Account Mapper
<code>org.forgerock.openam.authentication.modules.common.mapping.AccountProvider</code> interface.
String constructor parameters can be provided by appending | separated values.",
     "propertyOrder" : 1200,
     "type" : "string",
     "exampleValue" : ""
   },
   "clientSecret" : {
     "title" : "Client Secret",
     "description" : "OAuth client_secret parameter <p>For more information on the OAuth client_id
parameter refer to the RFC 6749 (http://tools.ietf.org/html/rfc6749#section-2.3.1), section 2.3.1.",
     "propertyOrder" : 200,
     "type" : "string",
     "format" : "password",
     "exampleValue" : ""
```

```
    }
  },
  "required" : [ "scopeString", "cfgAttributeMappingClasses", "cfgMixUpMitigation",
 "cfgAttributeMappingConfiguration", "scopeDelimiter", "issuer", "userInfoEndpoint", "redirectURI",
 "authenticationIdKey", "cfgAccountMapperConfiguration", "provider", "saveUserAttributesToSession",
 "tokenEndpoint", "authorizeEndpoint", "basicAuth", "clientSecret", "cfgAccountProviderClass",
 "clientId", "cfgAccountMapperClass" ]
}
```

OAuth2Client

Realm Operations

Resource path: `/realm-config/services/SocialIdentityProviders/oauth2Config`

Resource version: `1.0`

create

Usage:

```
am> create OAuth2Client --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "transform" : {
      "title" : "Transform Script",
      "description" : "A script that takes the raw profile object as input and outputs the normalized
 profile object.",
      "propertyOrder" : 10000,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "clientId" : {
      "title" : "Client ID",
      "description" : "OAuth client_id parameter<p> For more information on the OAuth client_id
 parameter refer to the RFC 6749 (http://tools.ietf.org/html/rfc6749#section-2.3.1), section 2.3.1.",
      "propertyOrder" : 200,
      "required" : true,
```

```
      "type" : "string",
      "exampleValue" : ""
    },
    "uiConfig" : {
      "title" : "UI Config Properties",
      "description" : "Mapping of display properties to be defined and consumed by the UI.",
      "propertyOrder" : 9999,
      "required" : true,
      "patternProperties" : {
        ".*" : {
          "type" : "string"
        }
      },
      "type" : "object",
      "exampleValue" : ""
    },
    "scopeDelimiter" : {
      "title" : "Scope Delimiter",
      "description" : "The delimiter used by an auth server to separate scopes.",
      "propertyOrder" : 800,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "scopes" : {
      "title" : "OAuth Scopes",
      "description" : "List of user profile properties<p>According to the OAuth 2.0 Authorization
Framework that the client application requires. The list depends on the permissions that the resource
owner grants to the client application. Some authorization servers use non-standard separators for
scopes.",
      "propertyOrder" : 900,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "minItems" : 1,
      "type" : "array",
      "exampleValue" : ""
    },
    "enabled" : {
      "title" : "Enabled",
      "description" : "",
      "propertyOrder" : 1,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "basicAuth" : {
      "title" : "Use Basic Auth",
      "description" : "When enabled, the client will use basic auth for authenticating with the social
auth provider. Enabled by default.",
      "propertyOrder" : 1000,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "redirectURI" : {
      "title" : "Redirect URL",
      "description" : "",
```

```
      "propertyOrder" : 700,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "authorizationEndpoint" : {
      "title" : "Authentication Endpoint URL",
      "description" : "OAuth authentication endpoint URL <p> This is the URL endpoint for OAuth
 authentication provided by the OAuth Identity Provider.",
      "propertyOrder" : 400,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "userInfoEndpoint" : {
      "title" : "User Profile Service URL",
      "description" : "User profile information URL <p> This URL endpoint provides user profile
 information and is provided by the OAuth Identity Provider NB This URL should return JSON objects in
 response.",
      "propertyOrder" : 600,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "tokenEndpoint" : {
      "title" : "Access Token Endpoint URL",
      "description" : "OAuth access token endpoint URL This is the URL endpoint for access token
 retrieval provided by the OAuth Identity Provider.Refer to the RFC 6749 (http://tools.ietf.org/html/
rfc6749#section-3.2), section 3.2.",
      "propertyOrder" : 500,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "authenticationIdKey" : {
      "title" : "Auth ID Key",
      "description" : "Field used to identify a user by the social provider.",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "exampleValue" : "sub"
    },
    "clientSecret" : {
      "title" : "Client Secret",
      "description" : "OAuth client_secret parameter <p>For more information on the OAuth client_id
 parameter refer to the RFC 6749 (http://tools.ietf.org/html/rfc6749#section-2.3.1), section 2.3.1.",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "string",
      "format" : "password",
      "exampleValue" : ""
    },
    "pkceMethod" : {
      "title" : "PKCE Method",
      "description" : "The PKCE transformation method to use when making requests to the authorization
 endpoint.",
      "propertyOrder" : 1100,
      "required" : true,
      "type" : "string",
```

```
      "exampleValue" : ""
    }
  }
}
```

delete

Usage:

```
am> delete OAuth2Client --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action OAuth2Client --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action OAuth2Client --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action OAuth2Client --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query OAuth2Client --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read OAuth2Client --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update OAuth2Client --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "transform" : {
      "title" : "Transform Script",
      "description" : "A script that takes the raw profile object as input and outputs the normalized
 profile object.",
      "propertyOrder" : 10000,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "clientId" : {
      "title" : "Client ID",
      "description" : "OAuth client_id parameter<p> For more information on the OAuth client_id
 parameter refer to the RFC 6749 (http://tools.ietf.org/html/rfc6749#section-2.3.1), section 2.3.1.",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "uiConfig" : {
```

```
      "title" : "UI Config Properties",
      "description" : "Mapping of display properties to be defined and consumed by the UI.",
      "propertyOrder" : 9999,
      "required" : true,
      "patternProperties" : {
        ".*" : {
          "type" : "string"
        }
      },
      "type" : "object",
      "exampleValue" : ""
    },
    "scopeDelimiter" : {
      "title" : "Scope Delimiter",
      "description" : "The delimiter used by an auth server to separate scopes.",
      "propertyOrder" : 800,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "scopes" : {
      "title" : "OAuth Scopes",
      "description" : "List of user profile properties<p>According to the OAuth 2.0 Authorization
Framework that the client application requires. The list depends on the permissions that the resource
owner grants to the client application. Some authorization servers use non-standard separators for
scopes.",
      "propertyOrder" : 900,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "minItems" : 1,
      "type" : "array",
      "exampleValue" : ""
    },
    "enabled" : {
      "title" : "Enabled",
      "description" : "",
      "propertyOrder" : 1,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "basicAuth" : {
      "title" : "Use Basic Auth",
      "description" : "When enabled, the client will use basic auth for authenticating with the social
auth provider. Enabled by default.",
      "propertyOrder" : 1000,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "redirectURI" : {
      "title" : "Redirect URL",
      "description" : "",
      "propertyOrder" : 700,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
```

```
    },
    "authorizationEndpoint" : {
      "title" : "Authentication Endpoint URL",
      "description" : "OAuth authentication endpoint URL <p> This is the URL endpoint for OAuth
 authentication provided by the OAuth Identity Provider.",
      "propertyOrder" : 400,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "userInfoEndpoint" : {
      "title" : "User Profile Service URL",
      "description" : "User profile information URL <p> This URL endpoint provides user profile
 information and is provided by the OAuth Identity Provider NB This URL should return JSON objects in
 response.",
      "propertyOrder" : 600,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "tokenEndpoint" : {
      "title" : "Access Token Endpoint URL",
      "description" : "OAuth access token endpoint URL This is the URL endpoint for access token
 retrieval provided by the OAuth Identity Provider.Refer to the RFC 6749 (http://tools.ietf.org/html/
rfc6749#section-3.2), section 3.2.",
      "propertyOrder" : 500,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "authenticationIdKey" : {
      "title" : "Auth ID Key",
      "description" : "Field used to identify a user by the social provider.",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "exampleValue" : "sub"
    },
    "clientSecret" : {
      "title" : "Client Secret",
      "description" : "OAuth client_secret parameter <p>For more information on the OAuth client_id
 parameter refer to the RFC 6749 (http://tools.ietf.org/html/rfc6749#section-2.3.1), section 2.3.1.",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "string",
      "format" : "password",
      "exampleValue" : ""
    },
    "pkceMethod" : {
      "title" : "PKCE Method",
      "description" : "The PKCE transformation method to use when making requests to the authorization
 endpoint.",
      "propertyOrder" : 1100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }
```

```
}
```

OAuth2ClientAgentGroups

Realm Operations

Agent Groups handler that is responsible for managing agent groups

Resource path: `/realm-config/agents/groups/OAuth2Client`

Resource version: `1.0`

create

Usage:

```
am> create OAuth2ClientAgentGroups --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "advancedOAuth2ClientConfig" : {
      "type" : "object",
      "title" : "Advanced",
      "propertyOrder" : 1,
      "properties" : {
        "grantTypes" : {
          "title" : "Grant Types",
          "description" : "The set of Grant Types (OAuth2 Flows) that are permitted to be used by this
 client.<br><br>If no Grant Types (OAuth2 Flows) are configured then AUTHORIZATION_CODE flow would be
 permitted by default.",
          "propertyOrder" : 23800,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "javascriptOrigins" : {
          "title" : "JavaScript Origins",
          "description" : "",
```

```
          "propertyOrder" : 23650,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "responseTypes" : {
          "title" : "Response Types",
          "description" : "Response types this client will support and use.",
          "propertyOrder" : 23800,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "contacts" : {
          "title" : "Contacts",
          "description" : "Email addresses of users who can administrate this client.",
          "propertyOrder" : 23900,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "sectorIdentifierUri" : {
          "title" : "Sector Identifier URI",
          "description" : "The Host component of this URL is used in the computation of pairwise
Subject Identifiers.",
          "propertyOrder" : 24300,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "requestUris" : {
          "title" : "Request uris",
          "description" : "Array of request_uri values that are pre-registered by the RP for use at
the OP.<br><br>The entire Request URI MUST NOT exceed 512 ASCII characters and MUST use either HTTP
or HTTPS. Otherwise the value will be ignored.",
          "propertyOrder" : 23700,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "isConsentImplied" : {
          "title" : "Implied consent",
          "description" : "When enabled, the resource owner will not be asked for consent during
authorization flows. The OAuth2 Provider must be configured to allow clients to skip consent.",
          "propertyOrder" : 26200,
          "required" : true,
          "type" : "boolean",
```

```
          "exampleValue" : ""
        },
        "policyUri" : {
          "title" : "Privacy Policy URI",
          "description" : "The URI for the client's privacy policy, for use in user-facing consent
 pages.",
          "propertyOrder" : 25375,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "name" : {
          "title" : "Display name",
          "description" : "A client name that may be relevant to the resource owner when considering
 approval.<br><br>The name may be entered as a single string or as pipe separated strings for
 locale and localized name; e.g. \"en|The ExampleCo Intranet\". Locale strings are in the format
 <code>language + \"_\" + country + \"_\" + variant</code>, e.g. en, en_GB, en_US_WIN. If the locale
 is omitted, the name is displayed to all users having undefined locales. e.g. \"The ExampleCo
 Intranet\".",
          "propertyOrder" : 23500,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "mixUpMitigation" : {
          "title" : "OAuth 2.0 Mix-Up Mitigation enabled",
          "description" : "Enables OAuth 2.0 mix-up mitigation on the authorization server
 side.<br><br>Enable this setting only if this OAuth 2.0 client supports the <a href=\"https://
tools.ietf.org/html/draft-ietf-oauth-mix-up-mitigation-01\">OAuth 2.0 Mix-Up Mitigation draft</a>,
 otherwise AM will fail to validate access token requests received from this client.",
          "propertyOrder" : 26300,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "tokenEndpointAuthMethod" : {
          "title" : "Token Endpoint Authentication Method",
          "description" : "The authentication method with which a client authenticates to the
 authorization server at the token endpoint. The authentication method applies to OIDC requests with
 the openid scope.",
          "propertyOrder" : 24000,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "descriptions" : {
          "title" : "Display description",
          "description" : "A description of the client or other information that may be relevant
 to the resource owner when considering approval.<br><br>The description may be entered as a single
 string or as pipe separated strings for locale and localized name; e.g. \"en|The company intranet
 is requesting the following access permission\". Locale strings are in the format <code>language
 + \"_\" + country + \"_\" + variant</code>, e.g. en, en_GB, en_US_WIN. If the locale is omitted,
```

```
the description is displayed to all users having undefined locales. e.g. \"The company intranet is
requesting the following access permission\".",
         "propertyOrder" : 23600,
         "required" : false,
         "items" : {
           "type" : "string"
         },
         "type" : "array",
         "exampleValue" : ""
       },
       "clientUri" : {
         "title" : "Client URI",
         "description" : "The URI for finding further information about the client from user-facing
UIs.",
         "propertyOrder" : 25325,
         "required" : false,
         "items" : {
           "type" : "string"
         },
         "type" : "array",
         "exampleValue" : ""
       },
       "logoUri" : {
         "title" : "Logo URI",
         "description" : "The URI for the client's logo, for use in user-facing UIs such as consent
pages and application pages.",
         "propertyOrder" : 25350,
         "required" : false,
         "items" : {
           "type" : "string"
         },
         "type" : "array",
         "exampleValue" : ""
       },
       "updateAccessToken" : {
         "title" : "Access Token",
         "description" : "The access token used to update the client.",
         "propertyOrder" : 25100,
         "required" : false,
         "type" : "string",
         "exampleValue" : ""
       },
       "subjectType" : {
         "title" : "Subject Type",
         "description" : "The subject type added to responses for this client. This value must be
included in \"Subject Type Supported\" in OAuth2Provider service setting.",
         "propertyOrder" : 24400,
         "required" : true,
         "type" : "string",
         "exampleValue" : ""
       }
     }
   },
   "signEncOAuth2ClientConfig" : {
     "type" : "object",
     "title" : "Signing and Encryption",
     "propertyOrder" : 3,
     "properties" : {
       "idTokenEncryptionAlgorithm" : {
```

```
          "title" : "ID Token Encryption Algorithm",
          "description" : "Algorithm the ID Token for this client must be encrypted with.",
          "propertyOrder" : 24700,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "userinfoSignedResponseAlg" : {
          "title" : "User info signed response algorithm",
          "description" : "JWS algorithm for signing UserInfo Responses. If this is specified, the
 response will be JWT <a href=\"https://tools.ietf.org/html/rfc7519\">JWT</a> serialized, and signed
 using JWS. The default, if omitted, is for the UserInfo Response to return the Claims as a UTF-8
 encoded JSON object using the application/json content-type.",
          "propertyOrder" : 27200,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "tokenIntrospectionResponseFormat" : {
          "title" : "Token introspection response format",
          "description" : "The token introspection endpoint offers different output format. see
 https://tools.ietf.org/html/draft-ietf-oauth-jwt-introspection-response-03",
          "propertyOrder" : 27800,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "clientJwtPublicKey" : {
          "title" : "Client JWT Bearer Public Key",
          "description" : "A Base64 encoded X509 certificate, containing the public key, represented
 as a UTF-8 PEM file, of the key pair for signing the Client Bearer JWT.",
          "propertyOrder" : 25400,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "tokenIntrospectionSignedResponseAlg" : {
          "title" : "Token introspection response signing algorithm",
          "description" : "Algorithm used for signing the introspection JWT response.",
          "propertyOrder" : 27810,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "userinfoResponseFormat" : {
          "title" : "User info response format.",
          "description" : "The user info endpoint offers different output format. See http://
openid.net/specs/openid-connect-core-1_0.html#UserInfoResponse",
          "propertyOrder" : 27100,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "requestParameterEncryptedEncryptionAlgorithm" : {
          "title" : "Request parameter encryption method",
          "description" : "JWE enc algorithm for encrypting the request parameter.<br><br>AM supports
 the following token encryption algorithms:<ul><li><code>A128GCM</code>, <code>A192GCM</code>,
 and <code>A256GCM</code> - AES in Galois Counter Mode (GCM) authenticated encryption mode.</
```

```
li><li><code>A128CBC-HS256</code>, <code>A192CBC-HS384</code>, and <code>A256CBC-HS512</code> - AES
 encryption in CBC mode, with HMAC-SHA-2 for integrity.</li></ul>",
          "propertyOrder" : 27700,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "tokenIntrospectionEncryptedResponseEncryptionAlgorithm" : {
          "title" : "Token introspection encrypted response encryption algorithm",
          "description" : "JWE 'enc' algorithm REQUIRED for encrypting token introspection responses.
 Sets the algorithm that will be used to encrypt the Plaintext of a JWE when the chosen introspection
 response format is 'signed then encrypted'.",
          "propertyOrder" : 27830,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "jwksUri" : {
          "title" : "Json Web Key URI",
          "description" : "The uri that contains the client's public keys in Json Web Key format.",
          "propertyOrder" : 24100,
          "required" : false,
          "type" : "string",
          "exampleValue" : "https://{{jwks-www}}/oauth2/{{realm}}/connect/jwk_uri"
        },
        "tokenIntrospectionEncryptedResponseAlg" : {
          "title" : "Token introspection response encryption algorithm",
          "description" : "JWE \"alg\" algorithm REQUIRED for encrypting introspection responses. Sets
 the algorithm that will be used to encrypt the Content Encryption Key when the chosen introspection
 response format is 'signed then encrypted'.",
          "propertyOrder" : 27820,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "requestParameterSignedAlg" : {
          "title" : "Request parameter signing algorithm",
          "description" : "JWS algorithm for signing the request parameter.",
          "propertyOrder" : 27500,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "mTLSSubjectDN" : {
          "title" : "mTLS Subject DN",
          "description" : "Expected Subject DN of certificate used for mTLS client certificate
 authentication. Defaults to CN=&lt;client_id&gt;. Only applicable when using CA-signed
 certificates.",
          "propertyOrder" : 25406,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "jwkStoreCacheMissCacheTime" : {
          "title" : "JWKs URI content cache miss cache time",
          "description" : "To avoid loading the JWKS URI content for every token signature
 verification, especially when the kid is not in the jwks content already cached, the JWKS content
 will be cache for a minimum period of time. This cache miss cache time defines the minimum of time
 the JWKS URI content is cache.",
```

```
          "propertyOrder" : 24120,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "idTokenSignedResponseAlg" : {
          "title" : "ID Token Signing Algorithm",
          "description" : "Algorithm the ID Token for this client must be signed with.",
          "propertyOrder" : 24500,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "userinfoEncryptedResponseEncryptionAlgorithm" : {
          "title" : "User info encrypted response encryption algorithm",
          "description" : "JWE enc algorithm for encrypting UserInfo Responses. If userinfo encrypted
 response algorithm is specified, the default for this value is A128CBC-HS256. When user info
 encrypted response encryption is included, user info encrypted response algorithm MUST also be
 provided.<br><br>AM supports the following token encryption algorithms:<ul><li><code>A128GCM</code>,
 <code>A192GCM</code>, and <code>A256GCM</code> - AES in Galois Counter Mode (GCM) authenticated
 encryption mode.</li><li><code>A128CBC-HS256</code>, <code>A192CBC-HS384</code>, and <code>A256CBC-
HS512</code> - AES encryption in CBC mode, with HMAC-SHA-2 for integrity.</li></ul>",
          "propertyOrder" : 27400,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "tokenEndpointAuthSigningAlgorithm" : {
          "title" : "Token Endpoint Authentication Signing Algorithm",
          "description" : "The JWS algorithm that MUST be used for signing the JWT used to
 authenticate the Client at the Token Endpointfor the private_key_jwt and client_secret_jwt
 authentication methods. All Token Requests using these authentication methods from this Client MUST
 be rejected, if the JWT is not signed with this algorithm.",
          "propertyOrder" : 24130,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "publicKeyLocation" : {
          "title" : "Public key selector",
          "description" : "Select the public key for this client to come from either the jwks_uri,
 manual jwks or X509 field.",
          "propertyOrder" : 25700,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "idTokenEncryptionEnabled" : {
          "title" : "Enable ID Token Encryption",
          "description" : "Select to enable ID token encryption.",
          "propertyOrder" : 24600,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "jwksCacheTimeout" : {
          "title" : "JWKs URI content cache timeout in ms",
```

```
          "description" : "To avoid loading the JWKS URI content for every token encryption, the JWKS
content is cached. This timeout defines the maximum of time the JWKS URI content can be cached before
being refreshed.",
          "propertyOrder" : 24110,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "userinfoEncryptedResponseAlg" : {
          "title" : "User info encrypted response algorithm",
          "description" : "JWE algorithm for encrypting UserInfo Responses. If both signing and
encryption are requested, the response will be signed then encrypted, with the result being a Nested
JWT. The default, if omitted, is that no encryption is performed.",
          "propertyOrder" : 27300,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "mTLSCertificateBoundAccessTokens" : {
          "title" : "Use Certificate-Bound Access Tokens",
          "description" : "Whether access tokens issued to this client should be bound to the X.509
certificate it uses to authenticate to the token endpoint. If enabled (and the provider supports it)
then an x5t#S256 confirmation key will be added to all access tokens with the SHA-256 hash of the
client's certificate.",
          "propertyOrder" : 25507,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "mTLSTrustedCert" : {
          "title" : "mTLS Self-Signed Certificate",
          "description" : "Self-signed PEM-encoded X.509 certificate for mTLS client certificate
authentication.",
          "propertyOrder" : 25405,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "jwkSet" : {
          "title" : "Json Web Key",
          "description" : "Raw JSON Web Key value containing the client's public keys.",
          "propertyOrder" : 24200,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "idTokenEncryptionMethod" : {
          "title" : "ID Token Encryption Method",
          "description" : "Encryption method the ID Token for this client must be encrypted with.",
          "propertyOrder" : 24800,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "requestParameterEncryptedAlg" : {
          "title" : "Request parameter encryption algorithm",
          "description" : "JWE algorithm for encrypting the request parameter.",
          "propertyOrder" : 27600,
          "required" : false,
```

```
          "type" : "string",
          "exampleValue" : ""
        },
        "idTokenPublicEncryptionKey" : {
          "title" : "Client ID Token Public Encryption Key",
          "description" : "A Base64 encoded public key for encrypting ID Tokens.",
          "propertyOrder" : 24900,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "coreOAuth2ClientConfig" : {
      "type" : "object",
      "title" : "Core",
      "propertyOrder" : 0,
      "properties" : {
        "loopbackInterfaceRedirection" : {
          "title" : "Allow wildcard ports in redirect URIs",
          "description" : "This flag indicates whether wildcards can be used for port numbers in
 redirect URIs. When this toggle is set to true and a wildcard is used the only allowed combinations
 of protocols and hosts are: http://127.0.0.1, https://127.0.0.1, http://[::1], https://[::1],
 http://localhost, https://localhost The wild cards are permitted only for the port values. For
 example - <code>http://localhost:80*</code>, <code>http://localhost:80?0/{path}</code>, <code>http://
localhost:80[8-9]0/{path}</code>",
          "propertyOrder" : 23150,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "clientName" : {
          "title" : "Client Name",
          "description" : "This value is a readable name for this client.",
          "propertyOrder" : 25300,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "status" : {
          "title" : "Status",
          "description" : "Status of the agent configuration.",
          "propertyOrder" : 200,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "authorizationCodeLifetime" : {
          "title" : "Authorization Code Lifetime (seconds)",
          "description" : "The time in seconds an authorization code is valid for. <i>NB</i> If this
 field is set to zero, Authorization Code Lifetime of the OAuth2 Provider is used instead of.",
          "propertyOrder" : 25800,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
```

```
        "accessTokenLifetime" : {
          "title" : "Access Token Lifetime (seconds)",
          "description" : "The time in seconds an access token is valid for. <i>NB</i> If this field
 is set to zero, Access Token Lifetime of the OAuth2 Provider is used instead of.",
          "propertyOrder" : 26000,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "clientType" : {
          "title" : "Client type",
          "description" : "Type of OAuth 2.0 client. Confidential clients can keep their password
 secret, and are typically web apps or other server-based clients. Public clients run the risk
 of exposing their password to a host or user agent, such as rich browser applications or desktop
 clients.",
          "propertyOrder" : 23100,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "redirectionUris" : {
          "title" : "Redirection URIs",
          "description" : "Redirection URIs (optional for confidential clients). Complete URIs or URIs
 consisting of protocol + authority + path are registered so that the OAuth 2.0 provider can trust
 that tokens are sent to trusted entities. If multiple URI's are registered, the client MUST specify
 the URI that the user should be redirected to following approval. May not contain a fragment (#).",
          "propertyOrder" : 23200,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "refreshTokenLifetime" : {
          "title" : "Refresh Token Lifetime (seconds)",
          "description" : "The time in seconds a refresh token is valid for. <i>NB</i> If this field
 is set to zero, Refresh Token Lifetime of the OAuth2 Provider is used instead. If this field is set
 to -1, the token will never expire.",
          "propertyOrder" : 25900,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "defaultScopes" : {
          "title" : "Default Scope(s)",
          "description" : "Default Scope(s). Scopes automatically given to tokens.<br><br>Default
 Scopes may be entered as simple strings or pipe separated strings representing the internal scope
 name, locale, and localized description; e.g. \"read|en|Permission to view email messages in your
 account\". Locale strings are in the format <code>language + \"_\" + country + \"_\" + variant</
code>, e.g. en, en_GB, en_US_WIN. If the locale and pipe is omitted, the description is displayed to
 all users having undefined locales. e.g. \"read|Permission to view email messages in your account
\". <i>NB</i> If the description is also omitted, nothing is displayed to all users, e.g. specifying
 \"read|\" would allow the scope \"read\" to be used by the client, but would not display it to the
 user when it was requested.",
          "propertyOrder" : 23700,
          "required" : false,
          "items" : {
            "type" : "string"
```

```
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "scopes" : {
          "title" : "Scope(s)",
          "description" : "Scope(s). Scopes are strings that are presented to the user for approval
 and included in tokens so that the protected resource may make decisions about what to give access
 to.<br><br>Scopes may be entered as simple strings or pipe separated strings representing the
 internal scope name, locale, and localized description; e.g. \"read|en|Permission to view email
 messages in your account\". Locale strings are in the format <code>language + \"_\" + country + \"_
\" + variant</code>, e.g. en, en_GB, en_US_WIN. If the locale and pipe is omitted, the description
 is displayed to all users having undefined locales. e.g. \"read|Permission to view email messages in
 your account\". <i>NB</i> If the description is also omitted, nothing is displayed to all users, e.g.
 specifying \"read|\" would allow the scope \"read\" to be used by the client, but would not display
 it to the user when it was requested.",
          "propertyOrder" : 23300,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        }
      }
    },
    "coreOpenIDClientConfig" : {
      "type" : "object",
      "title" : "OpenID Connect",
      "propertyOrder" : 2,
      "properties" : {
        "defaultMaxAge" : {
          "title" : "Default Max Age",
          "description" : "Minimum value 1. Sets the maximum length of time in seconds a session
 may be active after the authorization service has succeeded before the user must actively re-
authenticate.",
          "propertyOrder" : 25500,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "clientSessionUri" : {
          "title" : "Client Session URI",
          "description" : "This is the URI that will be used to check messages sent to the session
 management endpoints. This URI must match the origin of the message",
          "propertyOrder" : 25200,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "defaultMaxAgeEnabled" : {
          "title" : "Default Max Age Enabled",
          "description" : "Whether or not the default max age is enforced.",
          "propertyOrder" : 25600,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "claims" : {
```

```
          "title" : "Claim(s)",
          "description" : "List of claim name translations, which will override those specified for
the AS. Claims are values that are presented to the user to inform them what data is being made
available to the Client.<br><br>Claims may be entered as simple strings or pipe separated strings
representing the internal claim name, locale, and localized description; e.g. \"name|en|Your full
name\". Locale strings are in the format <code>language + \"_\" + country + \"_\" + variant</code>,
e.g. en, en_GB, en_US_WIN. If the locale and pipe is omitted, the description is displayed to all
users having undefined locales. e.g. \"name|Your full name\". <i>NB</i> If the description is also
omitted, nothing is displayed to all users, e.g. specifying \"name|\" would allow the claim \"name\"
to be used by the client, but would not display it to the user when it was requested.<p>If a value is
not given here, the value will be computed from the OAuth 2 Provider settings.</p>",
          "propertyOrder" : 23400,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "defaultAcrValues" : {
          "title" : "Default ACR values",
          "description" : "Default requested Authentication Context Class Reference
values.<br><br>Array of strings that specifies the default acr values that the OP is being requested
to use for processing requests from this Client, with the values appearing in order of preference.
The Authentication Context Class satisfied by the authentication performed is returned as the
acr Claim Value in the issued ID Token. The acr Claim is requested as a Voluntary Claim by this
parameter. The acr_values_supported discovery element contains a list of the acr values supported by
this server. Values specified in the acr_values request parameter or an individual acr Claim request
override these default values.",
          "propertyOrder" : 25650,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "jwtTokenLifetime" : {
          "title" : "OpenID Connect JWT Token Lifetime (seconds)",
          "description" : "The time in seconds a JWT is valid for. <i>NB</i> If this field is set to
zero, JWT Token Lifetime of the OAuth2 Provider is used instead of.",
          "propertyOrder" : 26100,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "postLogoutRedirectUri" : {
          "title" : "Post Logout Redirect URIs",
          "description" : "URIs that can be redirected to after the client logout process.",
          "propertyOrder" : 25000,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        }
      }
    },
```

```
    "coreUmaClientConfig" : {
      "type" : "object",
      "title" : "UMA",
      "propertyOrder" : 4,
      "properties" : {
        "claimsRedirectionUris" : {
          "title" : "Claims Redirection URIs",
          "description" : "Redirection URIs for returning to the client from UMA claims collection
 (not yet supported). If multiple URIs are registered, the client MUST specify the URI that the user
 should be redirected to following approval. May not contain a fragment (#).",
          "propertyOrder" : 23200,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        }
      }
    }
  }
}
```

delete

Usage:

```
am> delete OAuth2ClientAgentGroups --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action OAuth2ClientAgentGroups --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action OAuth2ClientAgentGroups --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action OAuth2ClientAgentGroups --realm Realm --actionName nextdescendents
```

query

Querying the agent groups of a specific type

Usage:

```
am> query OAuth2ClientAgentGroups --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read OAuth2ClientAgentGroups --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update OAuth2ClientAgentGroups --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "advancedOAuth2ClientConfig" : {
      "type" : "object",
      "title" : "Advanced",
      "propertyOrder" : 1,
      "properties" : {
        "grantTypes" : {
          "title" : "Grant Types",
          "description" : "The set of Grant Types (OAuth2 Flows) that are permitted to be used by this
 client.<br><br>If no Grant Types (OAuth2 Flows) are configured then AUTHORIZATION_CODE flow would be
 permitted by default.",
          "propertyOrder" : 23800,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "javascriptOrigins" : {
          "title" : "JavaScript Origins",
          "description" : "",
          "propertyOrder" : 23650,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "responseTypes" : {
          "title" : "Response Types",
          "description" : "Response types this client will support and use.",
          "propertyOrder" : 23800,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "contacts" : {
          "title" : "Contacts",
          "description" : "Email addresses of users who can administrate this client.",
          "propertyOrder" : 23900,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "sectorIdentifierUri" : {
```

```
          "title" : "Sector Identifier URI",
          "description" : "The Host component of this URL is used in the computation of pairwise
Subject Identifiers.",
          "propertyOrder" : 24300,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "requestUris" : {
          "title" : "Request uris",
          "description" : "Array of request_uri values that are pre-registered by the RP for use at
the OP.<br><br>The entire Request URI MUST NOT exceed 512 ASCII characters and MUST use either HTTP
or HTTPS. Otherwise the value will be ignored.",
          "propertyOrder" : 23700,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "isConsentImplied" : {
          "title" : "Implied consent",
          "description" : "When enabled, the resource owner will not be asked for consent during
authorization flows. The OAuth2 Provider must be configured to allow clients to skip consent.",
          "propertyOrder" : 26200,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "policyUri" : {
          "title" : "Privacy Policy URI",
          "description" : "The URI for the client's privacy policy, for use in user-facing consent
pages.",
          "propertyOrder" : 25375,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "name" : {
          "title" : "Display name",
          "description" : "A client name that may be relevant to the resource owner when considering
approval.<br><br>The name may be entered as a single string or as pipe separated strings for
locale and localized name; e.g. \"en|The ExampleCo Intranet\". Locale strings are in the format
<code>language + \"_\" + country + \"_\" + variant</code>, e.g. en, en_GB, en_US_WIN. If the locale
is omitted, the name is displayed to all users having undefined locales. e.g. \"The ExampleCo
Intranet\".",
          "propertyOrder" : 23500,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "mixUpMitigation" : {
```

```
          "title" : "OAuth 2.0 Mix-Up Mitigation enabled",
          "description" : "Enables OAuth 2.0 mix-up mitigation on the authorization server
 side.<br><br>Enable this setting only if this OAuth 2.0 client supports the <a href=\"https://
tools.ietf.org/html/draft-ietf-oauth-mix-up-mitigation-01\">OAuth 2.0 Mix-Up Mitigation draft</a>,
 otherwise AM will fail to validate access token requests received from this client.",
          "propertyOrder" : 26300,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "tokenEndpointAuthMethod" : {
          "title" : "Token Endpoint Authentication Method",
          "description" : "The authentication method with which a client authenticates to the
 authorization server at the token endpoint. The authentication method applies to OIDC requests with
 the openid scope.",
          "propertyOrder" : 24000,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "descriptions" : {
          "title" : "Display description",
          "description" : "A description of the client or other information that may be relevant
 to the resource owner when considering approval.<br><br>The description may be entered as a single
 string or as pipe separated strings for locale and localized name; e.g. \"en|The company intranet
 is requesting the following access permission\". Locale strings are in the format <code>language
 + \"_\" + country + \"_\" + variant</code>, e.g. en, en_GB, en_US_WIN. If the locale is omitted,
 the description is displayed to all users having undefined locales. e.g. \"The company intranet is
 requesting the following access permission\".",
          "propertyOrder" : 23600,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "clientUri" : {
          "title" : "Client URI",
          "description" : "The URI for finding further information about the client from user-facing
 UIs.",
          "propertyOrder" : 25325,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "logoUri" : {
          "title" : "Logo URI",
          "description" : "The URI for the client's logo, for use in user-facing UIs such as consent
 pages and application pages.",
          "propertyOrder" : 25350,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
```

```
          "exampleValue" : ""
        },
        "updateAccessToken" : {
          "title" : "Access Token",
          "description" : "The access token used to update the client.",
          "propertyOrder" : 25100,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "subjectType" : {
          "title" : "Subject Type",
          "description" : "The subject type added to responses for this client. This value must be
included in \"Subject Type Supported\" in OAuth2Provider service setting.",
          "propertyOrder" : 24400,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "signEncOAuth2ClientConfig" : {
      "type" : "object",
      "title" : "Signing and Encryption",
      "propertyOrder" : 3,
      "properties" : {
        "idTokenEncryptionAlgorithm" : {
          "title" : "ID Token Encryption Algorithm",
          "description" : "Algorithm the ID Token for this client must be encrypted with.",
          "propertyOrder" : 24700,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "userinfoSignedResponseAlg" : {
          "title" : "User info signed response algorithm",
          "description" : "JWS algorithm for signing UserInfo Responses. If this is specified, the
response will be JWT <a href=\"https://tools.ietf.org/html/rfc7519\">JWT</a> serialized, and signed
using JWS. The default, if omitted, is for the UserInfo Response to return the Claims as a UTF-8
encoded JSON object using the application/json content-type.",
          "propertyOrder" : 27200,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "tokenIntrospectionResponseFormat" : {
          "title" : "Token introspection response format",
          "description" : "The token introspection endpoint offers different output format. see
https://tools.ietf.org/html/draft-ietf-oauth-jwt-introspection-response-03",
          "propertyOrder" : 27800,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "clientJwtPublicKey" : {
          "title" : "Client JWT Bearer Public Key",
          "description" : "A Base64 encoded X509 certificate, containing the public key, represented
as a UTF-8 PEM file, of the key pair for signing the Client Bearer JWT.",
          "propertyOrder" : 25400,
```

```
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "tokenIntrospectionSignedResponseAlg" : {
          "title" : "Token introspection response signing algorithm",
          "description" : "Algorithm used for signing the introspection JWT response.",
          "propertyOrder" : 27810,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "userinfoResponseFormat" : {
          "title" : "User info response format.",
          "description" : "The user info endpoint offers different output format. See http://
openid.net/specs/openid-connect-core-1_0.html#UserInfoResponse",
          "propertyOrder" : 27100,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "requestParameterEncryptedEncryptionAlgorithm" : {
          "title" : "Request parameter encryption method",
          "description" : "JWE enc algorithm for encrypting the request parameter.<br><br>AM supports
 the following token encryption algorithms:<ul><li><code>A128GCM</code>, <code>A192GCM</code>,
 and <code>A256GCM</code> - AES in Galois Counter Mode (GCM) authenticated encryption mode.</
li><li><code>A128CBC-HS256</code>, <code>A192CBC-HS384</code>, and <code>A256CBC-HS512</code> - AES
 encryption in CBC mode, with HMAC-SHA-2 for integrity.</li></ul>",
          "propertyOrder" : 27700,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "tokenIntrospectionEncryptedResponseEncryptionAlgorithm" : {
          "title" : "Token introspection encrypted response encryption algorithm",
          "description" : "JWE 'enc' algorithm REQUIRED for encrypting token introspection responses.
 Sets the algorithm that will be used to encrypt the Plaintext of a JWE when the chosen introspection
 response format is 'signed then encrypted'.",
          "propertyOrder" : 27830,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "jwksUri" : {
          "title" : "Json Web Key URI",
          "description" : "The uri that contains the client's public keys in Json Web Key format.",
          "propertyOrder" : 24100,
          "required" : false,
          "type" : "string",
          "exampleValue" : "https://{{jwks-www}}/oauth2/{{realm}}/connect/jwk_uri"
        },
        "tokenIntrospectionEncryptedResponseAlg" : {
          "title" : "Token introspection response encryption algorithm",
          "description" : "JWE \"alg\" algorithm REQUIRED for encrypting introspection responses. Sets
 the algorithm that will be used to encrypt the Content Encryption Key when the chosen introspection
 response format is 'signed then encrypted'.",
          "propertyOrder" : 27820,
          "required" : true,
          "type" : "string",
```

```
          "exampleValue" : ""
        },
        "requestParameterSignedAlg" : {
          "title" : "Request parameter signing algorithm",
          "description" : "JWS algorithm for signing the request parameter.",
          "propertyOrder" : 27500,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "mTLSSubjectDN" : {
          "title" : "mTLS Subject DN",
          "description" : "Expected Subject DN of certificate used for mTLS client certificate
 authentication. Defaults to CN=&lt;client_id&gt;. Only applicable when using CA-signed
 certificates.",
          "propertyOrder" : 25406,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "jwkStoreCacheMissCacheTime" : {
          "title" : "JWKs URI content cache miss cache time",
          "description" : "To avoid loading the JWKS URI content for every token signature
 verification, especially when the kid is not in the jwks content already cached, the JWKS content
 will be cache for a minimum period of time. This cache miss cache time defines the minimum of time
 the JWKS URI content is cache.",
          "propertyOrder" : 24120,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "idTokenSignedResponseAlg" : {
          "title" : "ID Token Signing Algorithm",
          "description" : "Algorithm the ID Token for this client must be signed with.",
          "propertyOrder" : 24500,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "userinfoEncryptedResponseEncryptionAlgorithm" : {
          "title" : "User info encrypted response encryption algorithm",
          "description" : "JWE enc algorithm for encrypting UserInfo Responses. If userinfo encrypted
 response algorithm is specified, the default for this value is A128CBC-HS256. When user info
 encrypted response encryption is included, user info encrypted response algorithm MUST also be
 provided.<br><br>AM supports the following token encryption algorithms:<ul><li><code>A128GCM</code>,
 <code>A192GCM</code>, and <code>A256GCM</code> - AES in Galois Counter Mode (GCM) authenticated
 encryption mode.</li><li><code>A128CBC-HS256</code>, <code>A192CBC-HS384</code>, and <code>A256CBC-
HS512</code> - AES encryption in CBC mode, with HMAC-SHA-2 for integrity.</li></ul>",
          "propertyOrder" : 27400,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "tokenEndpointAuthSigningAlgorithm" : {
          "title" : "Token Endpoint Authentication Signing Algorithm",
          "description" : "The JWS algorithm that MUST be used for signing the JWT used to
 authenticate the Client at the Token Endpointfor the private_key_jwt and client_secret_jwt
 authentication methods. All Token Requests using these authentication methods from this Client MUST
 be rejected, if the JWT is not signed with this algorithm.",
```

```
          "propertyOrder" : 24130,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "publicKeyLocation" : {
          "title" : "Public key selector",
          "description" : "Select the public key for this client to come from either the jwks_uri,
manual jwks or X509 field.",
          "propertyOrder" : 25700,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "idTokenEncryptionEnabled" : {
          "title" : "Enable ID Token Encryption",
          "description" : "Select to enable ID token encryption.",
          "propertyOrder" : 24600,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "jwksCacheTimeout" : {
          "title" : "JWKs URI content cache timeout in ms",
          "description" : "To avoid loading the JWKS URI content for every token encryption, the JWKS
content is cached. This timeout defines the maximum of time the JWKS URI content can be cached before
being refreshed.",
          "propertyOrder" : 24110,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "userinfoEncryptedResponseAlg" : {
          "title" : "User info encrypted response algorithm",
          "description" : "JWE algorithm for encrypting UserInfo Responses. If both signing and
encryption are requested, the response will be signed then encrypted, with the result being a Nested
JWT. The default, if omitted, is that no encryption is performed.",
          "propertyOrder" : 27300,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "mTLSCertificateBoundAccessTokens" : {
          "title" : "Use Certificate-Bound Access Tokens",
          "description" : "Whether access tokens issued to this client should be bound to the X.509
certificate it uses to authenticate to the token endpoint. If enabled (and the provider supports it)
then an x5t#S256 confirmation key will be added to all access tokens with the SHA-256 hash of the
client's certificate.",
          "propertyOrder" : 25507,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "mTLSTrustedCert" : {
          "title" : "mTLS Self-Signed Certificate",
          "description" : "Self-signed PEM-encoded X.509 certificate for mTLS client certificate
authentication.",
          "propertyOrder" : 25405,
          "required" : false,
```

```
          "type" : "string",
          "exampleValue" : ""
        },
        "jwkSet" : {
          "title" : "Json Web Key",
          "description" : "Raw JSON Web Key value containing the client's public keys.",
          "propertyOrder" : 24200,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "idTokenEncryptionMethod" : {
          "title" : "ID Token Encryption Method",
          "description" : "Encryption method the ID Token for this client must be encrypted with.",
          "propertyOrder" : 24800,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "requestParameterEncryptedAlg" : {
          "title" : "Request parameter encryption algorithm",
          "description" : "JWE algorithm for encrypting the request parameter.",
          "propertyOrder" : 27600,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "idTokenPublicEncryptionKey" : {
          "title" : "Client ID Token Public Encryption Key",
          "description" : "A Base64 encoded public key for encrypting ID Tokens.",
          "propertyOrder" : 24900,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "coreOAuth2ClientConfig" : {
      "type" : "object",
      "title" : "Core",
      "propertyOrder" : 0,
      "properties" : {
        "loopbackInterfaceRedirection" : {
          "title" : "Allow wildcard ports in redirect URIs",
          "description" : "This flag indicates whether wildcards can be used for port numbers in
 redirect URIs. When this toggle is set to true and a wildcard is used the only allowed combinations
 of protocols and hosts are: http://127.0.0.1, https://127.0.0.1, http://[::1], https://[::1],
 http://localhost, https://localhost The wild cards are permitted only for the port values. For
 example - <code>http://localhost:80*</code>, <code>http://localhost:80?0/{path}</code>, <code>http://
localhost:80[8-9]0/{path}</code>",
          "propertyOrder" : 23150,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "clientName" : {
          "title" : "Client Name",
          "description" : "This value is a readable name for this client.",
          "propertyOrder" : 25300,
```

```
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "status" : {
          "title" : "Status",
          "description" : "Status of the agent configuration.",
          "propertyOrder" : 200,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "authorizationCodeLifetime" : {
          "title" : "Authorization Code Lifetime (seconds)",
          "description" : "The time in seconds an authorization code is valid for. <i>NB</i> If this
field is set to zero, Authorization Code Lifetime of the OAuth2 Provider is used instead of.",
          "propertyOrder" : 25800,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "accessTokenLifetime" : {
          "title" : "Access Token Lifetime (seconds)",
          "description" : "The time in seconds an access token is valid for. <i>NB</i> If this field
is set to zero, Access Token Lifetime of the OAuth2 Provider is used instead of.",
          "propertyOrder" : 26000,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "clientType" : {
          "title" : "Client type",
          "description" : "Type of OAuth 2.0 client. Confidential clients can keep their password
secret, and are typically web apps or other server-based clients. Public clients run the risk
of exposing their password to a host or user agent, such as rich browser applications or desktop
clients.",
          "propertyOrder" : 23100,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "redirectionUris" : {
          "title" : "Redirection URIs",
          "description" : "Redirection URIs (optional for confidential clients). Complete URIs or URIs
consisting of protocol + authority + path are registered so that the OAuth 2.0 provider can trust
that tokens are sent to trusted entities. If multiple URI's are registered, the client MUST specify
the URI that the user should be redirected to following approval. May not contain a fragment (#).",
          "propertyOrder" : 23200,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "refreshTokenLifetime" : {
```

```
          "title" : "Refresh Token Lifetime (seconds)",
          "description" : "The time in seconds a refresh token is valid for. <i>NB</i> If this field
 is set to zero, Refresh Token Lifetime of the OAuth2 Provider is used instead. If this field is set
 to -1, the token will never expire.",
          "propertyOrder" : 25900,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "defaultScopes" : {
          "title" : "Default Scope(s)",
          "description" : "Default Scope(s). Scopes automatically given to tokens.<br><br>Default
 Scopes may be entered as simple strings or pipe separated strings representing the internal scope
 name, locale, and localized description; e.g. \"read|en|Permission to view email messages in your
 account\". Locale strings are in the format <code>language + \"_\" + country + \"_\" + variant</
code>, e.g. en, en_GB, en_US_WIN. If the locale and pipe is omitted, the description is displayed to
 all users having undefined locales. e.g. \"read|Permission to view email messages in your account
\". <i>NB</i> If the description is also omitted, nothing is displayed to all users, e.g. specifying
 \"read|\" would allow the scope \"read\" to be used by the client, but would not display it to the
 user when it was requested.",
          "propertyOrder" : 23700,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "scopes" : {
          "title" : "Scope(s)",
          "description" : "Scope(s). Scopes are strings that are presented to the user for approval
 and included in tokens so that the protected resource may make decisions about what to give access
 to.<br><br>Scopes may be entered as simple strings or pipe separated strings representing the
 internal scope name, locale, and localized description; e.g. \"read|en|Permission to view email
 messages in your account\". Locale strings are in the format <code>language + \"_\" + country + \"_
\" + variant</code>, e.g. en, en_GB, en_US_WIN. If the locale and pipe is omitted, the description
 is displayed to all users having undefined locales. e.g. \"read|Permission to view email messages in
 your account\". <i>NB</i> If the description is also omitted, nothing is displayed to all users, e.g.
 specifying \"read|\" would allow the scope \"read\" to be used by the client, but would not display
 it to the user when it was requested.",
          "propertyOrder" : 23300,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        }
      }
    },
    "coreOpenIDClientConfig" : {
      "type" : "object",
      "title" : "OpenID Connect",
      "propertyOrder" : 2,
      "properties" : {
        "defaultMaxAge" : {
          "title" : "Default Max Age",
```

```
          "description" : "Minimum value 1. Sets the maximum length of time in seconds a session
 may be active after the authorization service has succeeded before the user must actively re-
authenticate.",
          "propertyOrder" : 25500,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "clientSessionUri" : {
          "title" : "Client Session URI",
          "description" : "This is the URI that will be used to check messages sent to the session
 management endpoints. This URI must match the origin of the message",
          "propertyOrder" : 25200,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "defaultMaxAgeEnabled" : {
          "title" : "Default Max Age Enabled",
          "description" : "Whether or not the default max age is enforced.",
          "propertyOrder" : 25600,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "claims" : {
          "title" : "Claim(s)",
          "description" : "List of claim name translations, which will override those specified for
 the AS. Claims are values that are presented to the user to inform them what data is being made
 available to the Client.<br><br>Claims may be entered as simple strings or pipe separated strings
 representing the internal claim name, locale, and localized description; e.g. \"name|en|Your full
 name\". Locale strings are in the format <code>language + \"_\" + country + \"_\" + variant</code>,
 e.g. en, en_GB, en_US_WIN. If the locale and pipe is omitted, the description is displayed to all
 users having undefined locales. e.g. \"name|Your full name\". <i>NB</i> If the description is also
 omitted, nothing is displayed to all users, e.g. specifying \"name|\" would allow the claim \"name\"
 to be used by the client, but would not display it to the user when it was requested.<p>If a value is
 not given here, the value will be computed from the OAuth 2 Provider settings.</p>",
          "propertyOrder" : 23400,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "defaultAcrValues" : {
          "title" : "Default ACR values",
          "description" : "Default requested Authentication Context Class Reference
 values.<br><br>Array of strings that specifies the default acr values that the OP is being requested
 to use for processing requests from this Client, with the values appearing in order of preference.
 The Authentication Context Class satisfied by the authentication performed is returned as the
 acr Claim Value in the issued ID Token. The acr Claim is requested as a Voluntary Claim by this
 parameter. The acr_values_supported discovery element contains a list of the acr values supported by
 this server. Values specified in the acr_values request parameter or an individual acr Claim request
 override these default values.",
          "propertyOrder" : 25650,
          "required" : false,
          "items" : {
            "type" : "string"
```

```
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "jwtTokenLifetime" : {
          "title" : "OpenID Connect JWT Token Lifetime (seconds)",
          "description" : "The time in seconds a JWT is valid for. <i>NB</i> If this field is set to
 zero, JWT Token Lifetime of the OAuth2 Provider is used instead of.",
          "propertyOrder" : 26100,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "postLogoutRedirectUri" : {
          "title" : "Post Logout Redirect URIs",
          "description" : "URIs that can be redirected to after the client logout process.",
          "propertyOrder" : 25000,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        }
      }
    },
    "coreUmaClientConfig" : {
      "type" : "object",
      "title" : "UMA",
      "propertyOrder" : 4,
      "properties" : {
        "claimsRedirectionUris" : {
          "title" : "Claims Redirection URIs",
          "description" : "Redirection URIs for returning to the client from UMA claims collection
 (not yet supported). If multiple URIs are registered, the client MUST specify the URI that the user
 should be redirected to following approval. May not contain a fragment (#).",
          "propertyOrder" : 23200,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        }
      }
    }
  }
}
```


OAuth2Clients

Realm Operations

Agents handler that is responsible for managing agents

Resource path: `/realm-config/agents/OAuth2Client`

Resource version: `1.0`

create

Usage:

```
am> create OAuth2Clients --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "coreOAuth2ClientConfig" : {
      "type" : "object",
      "title" : "Core",
      "propertyOrder" : 0,
      "properties" : {
        "accessTokenLifetime" : {
          "title" : "Access Token Lifetime (seconds)",
          "description" : "The time in seconds an access token is valid for. <i>NB</i> If this field
 is set to zero, Access Token Lifetime of the OAuth2 Provider is used instead of.",
          "propertyOrder" : 26000,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "integer",
              "required" : true
            }
          }
        },
        "agentgroup" : {
          "title" : "Group",
          "description" : "Add the client to a group to allow inheritance of property values from the
 group. <br>Changing the group will update inherited property values. <br>Inherited property values
 are copied to the client.",
          "propertyOrder" : 100,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
```

```
        "clientName" : {
          "title" : "Client Name",
          "description" : "This value is a readable name for this client.",
          "propertyOrder" : 25300,
          "items" : {
            "type" : "string"
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "array",
              "required" : false
            }
          }
        },
        "userpassword" : {
          "title" : "Client secret",
          "description" : "Client secret. Used when the client authenticates to AM.",
          "propertyOrder" : 23000,
          "required" : true,
          "type" : "string",
          "format" : "password",
          "exampleValue" : ""
        },
        "authorizationCodeLifetime" : {
          "title" : "Authorization Code Lifetime (seconds)",
          "description" : "The time in seconds an authorization code is valid for. <i>NB</i> If this
 field is set to zero, Authorization Code Lifetime of the OAuth2 Provider is used instead of.",
          "propertyOrder" : 25800,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "integer",
              "required" : true
            }
          }
        },
        "loopbackInterfaceRedirection" : {
          "title" : "Allow wildcard ports in redirect URIs",
          "description" : "This flag indicates whether wildcards can be used for port numbers in
 redirect URIs. When this toggle is set to true and a wildcard is used the only allowed combinations
 of protocols and hosts are: http://127.0.0.1, https://127.0.0.1, http://[::1], https://[::1],
 http://localhost, https://localhost The wild cards are permitted only for the port values. For
 example - <code>http://localhost:80*</code>, <code>http://localhost:80?0/{path}</code>, <code>http://
localhost:80[8-9]0/{path}</code>",
          "propertyOrder" : 23150,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
```

```
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : false
            }
          }
        },
        "status" : {
          "title" : "Status",
          "description" : "Status of the agent configuration.",
          "propertyOrder" : 200,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : true
            }
          }
        },
        "clientType" : {
          "title" : "Client type",
          "description" : "Type of OAuth 2.0 client. Confidential clients can keep their password
secret, and are typically web apps or other server-based clients. Public clients run the risk
of exposing their password to a host or user agent, such as rich browser applications or desktop
clients.",
          "propertyOrder" : 23100,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : true
            }
          }
        },
        "refreshTokenLifetime" : {
          "title" : "Refresh Token Lifetime (seconds)",
          "description" : "The time in seconds a refresh token is valid for. <i>NB</i> If this field
is set to zero, Refresh Token Lifetime of the OAuth2 Provider is used instead. If this field is set
to -1, the token will never expire.",
          "propertyOrder" : 25900,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
```

```
            },
            "value" : {
              "type" : "integer",
              "required" : true
            }
          }
        },
        "scopes" : {
          "title" : "Scope(s)",
          "description" : "Scope(s). Scopes are strings that are presented to the user for approval
 and included in tokens so that the protected resource may make decisions about what to give access
 to.<br><br>Scopes may be entered as simple strings or pipe separated strings representing the
 internal scope name, locale, and localized description; e.g. \"read|en|Permission to view email
 messages in your account\". Locale strings are in the format <code>language + \"_\" + country + \"_
\" + variant</code>, e.g. en, en_GB, en_US_WIN. If the locale and pipe is omitted, the description
 is displayed to all users having undefined locales. e.g. \"read|Permission to view email messages in
 your account\". <i>NB</i> If the description is also omitted, nothing is displayed to all users, e.g.
 specifying \"read|\" would allow the scope \"read\" to be used by the client, but would not display
 it to the user when it was requested.",
          "propertyOrder" : 23300,
          "items" : {
            "type" : "string"
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "array",
              "required" : false
            }
          }
        },
        "redirectionUris" : {
          "title" : "Redirection URIs",
          "description" : "Redirection URIs (optional for confidential clients). Complete URIs or URIs
 consisting of protocol + authority + path are registered so that the OAuth 2.0 provider can trust
 that tokens are sent to trusted entities. If multiple URI's are registered, the client MUST specify
 the URI that the user should be redirected to following approval. May not contain a fragment (#).",
          "propertyOrder" : 23200,
          "items" : {
            "type" : "string"
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "array",
              "required" : false
            }
          }
        },
```

```
       "defaultScopes" : {
         "title" : "Default Scope(s)",
         "description" : "Default Scope(s). Scopes automatically given to tokens.<br><br>Default
 Scopes may be entered as simple strings or pipe separated strings representing the internal scope
 name, locale, and localized description; e.g. \"read|en|Permission to view email messages in your
 account\". Locale strings are in the format <code>language + \"_\" + country + \"_\" + variant</
code>, e.g. en, en_GB, en_US_WIN. If the locale and pipe is omitted, the description is displayed to
 all users having undefined locales. e.g. \"read|Permission to view email messages in your account
\". <i>NB</i> If the description is also omitted, nothing is displayed to all users, e.g. specifying
 \"read|\" would allow the scope \"read\" to be used by the client, but would not display it to the
 user when it was requested.",
         "propertyOrder" : 23700,
         "items" : {
           "type" : "string"
         },
         "type" : "object",
         "exampleValue" : "",
         "properties" : {
           "inherited" : {
             "type" : "boolean",
             "required" : true
           },
           "value" : {
             "type" : "array",
             "required" : false
           }
         }
       }
     }
   },
   "advancedOAuth2ClientConfig" : {
     "type" : "object",
     "title" : "Advanced",
     "propertyOrder" : 1,
     "properties" : {
       "isConsentImplied" : {
         "title" : "Implied consent",
         "description" : "When enabled, the resource owner will not be asked for consent during
 authorization flows. The OAuth2 Provider must be configured to allow clients to skip consent.",
         "propertyOrder" : 26200,
         "type" : "object",
         "exampleValue" : "",
         "properties" : {
           "inherited" : {
             "type" : "boolean",
             "required" : true
           },
           "value" : {
             "type" : "boolean",
             "required" : true
           }
         }
       },
       "subjectType" : {
         "title" : "Subject Type",
         "description" : "The subject type added to responses for this client. This value must be
 included in \"Subject Type Supported\" in OAuth2Provider service setting.",
         "propertyOrder" : 24400,
         "type" : "object",
```

```
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : true
            }
          }
        },
        "contacts" : {
          "title" : "Contacts",
          "description" : "Email addresses of users who can administrate this client.",
          "propertyOrder" : 23900,
          "items" : {
            "type" : "string"
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "array",
              "required" : false
            }
          }
        },
        "mixUpMitigation" : {
          "title" : "OAuth 2.0 Mix-Up Mitigation enabled",
          "description" : "Enables OAuth 2.0 mix-up mitigation on the authorization server
 side.<br><br>Enable this setting only if this OAuth 2.0 client supports the <a href=\"https://
tools.ietf.org/html/draft-ietf-oauth-mix-up-mitigation-01\">OAuth 2.0 Mix-Up Mitigation draft</a>,
 otherwise AM will fail to validate access token requests received from this client.",
          "propertyOrder" : 26300,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : true
            }
          }
        },
        "policyUri" : {
          "title" : "Privacy Policy URI",
          "description" : "The URI for the client's privacy policy, for use in user-facing consent
 pages.",
          "propertyOrder" : 25375,
          "items" : {
            "type" : "string"
```

```
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "array",
              "required" : false
            }
          }
        },
        "name" : {
          "title" : "Display name",
          "description" : "A client name that may be relevant to the resource owner when considering
approval.<br><br>The name may be entered as a single string or as pipe separated strings for
locale and localized name; e.g. \"en|The ExampleCo Intranet\". Locale strings are in the format
<code>language + \"_\" + country + \"_\" + variant</code>, e.g. en, en_GB, en_US_WIN. If the locale
is omitted, the name is displayed to all users having undefined locales. e.g. \"The ExampleCo
Intranet\".",
          "propertyOrder" : 23500,
          "items" : {
            "type" : "string"
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "array",
              "required" : false
            }
          }
        },
        "grantTypes" : {
          "title" : "Grant Types",
          "description" : "The set of Grant Types (OAuth2 Flows) that are permitted to be used by this
client.<br><br>If no Grant Types (OAuth2 Flows) are configured then AUTHORIZATION_CODE flow would be
permitted by default.",
          "propertyOrder" : 23800,
          "items" : {
            "type" : "string"
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "array",
              "required" : true
            }
```

```
        }
      },
      "updateAccessToken" : {
        "title" : "Access Token",
        "description" : "The access token used to update the client.",
        "propertyOrder" : 25100,
        "type" : "object",
        "exampleValue" : "",
        "properties" : {
          "inherited" : {
            "type" : "boolean",
            "required" : true
          },
          "value" : {
            "type" : "string",
            "required" : false
          }
        }
      },
      "descriptions" : {
        "title" : "Display description",
        "description" : "A description of the client or other information that may be relevant
to the resource owner when considering approval.<br><br>The description may be entered as a single
string or as pipe separated strings for locale and localized name; e.g. \"en|The company intranet
is requesting the following access permission\". Locale strings are in the format <code>language
+ \"_\" + country + \"_\" + variant</code>, e.g. en, en_GB, en_US_WIN. If the locale is omitted,
the description is displayed to all users having undefined locales. e.g. \"The company intranet is
requesting the following access permission\".",
        "propertyOrder" : 23600,
        "items" : {
          "type" : "string"
        },
        "type" : "object",
        "exampleValue" : "",
        "properties" : {
          "inherited" : {
            "type" : "boolean",
            "required" : true
          },
          "value" : {
            "type" : "array",
            "required" : false
          }
        }
      },
      "tokenEndpointAuthMethod" : {
        "title" : "Token Endpoint Authentication Method",
        "description" : "The authentication method with which a client authenticates to the
authorization server at the token endpoint. The authentication method applies to OIDC requests with
the openid scope.",
        "propertyOrder" : 24000,
        "type" : "object",
        "exampleValue" : "",
        "properties" : {
          "inherited" : {
            "type" : "boolean",
            "required" : true
          },
          "value" : {
```

```
              "type" : "string",
              "required" : true
            }
          }
        },
        "responseTypes" : {
          "title" : "Response Types",
          "description" : "Response types this client will support and use.",
          "propertyOrder" : 23800,
          "items" : {
            "type" : "string"
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "array",
              "required" : true
            }
          }
        },
        "javascriptOrigins" : {
          "title" : "JavaScript Origins",
          "description" : "",
          "propertyOrder" : 23650,
          "items" : {
            "type" : "string"
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "array",
              "required" : false
            }
          }
        },
        "clientUri" : {
          "title" : "Client URI",
          "description" : "The URI for finding further information about the client from user-facing
UIs.",
          "propertyOrder" : 25325,
          "items" : {
            "type" : "string"
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
```

```
            },
            "value" : {
              "type" : "array",
              "required" : false
            }
          }
        },
        "sectorIdentifierUri" : {
          "title" : "Sector Identifier URI",
          "description" : "The Host component of this URL is used in the computation of pairwise
Subject Identifiers.",
          "propertyOrder" : 24300,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "requestUris" : {
          "title" : "Request uris",
          "description" : "Array of request_uri values that are pre-registered by the RP for use at
the OP.<br><br>The entire Request URI MUST NOT exceed 512 ASCII characters and MUST use either HTTP
or HTTPS. Otherwise the value will be ignored.",
          "propertyOrder" : 23700,
          "items" : {
            "type" : "string"
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "array",
              "required" : false
            }
          }
        },
        "logoUri" : {
          "title" : "Logo URI",
          "description" : "The URI for the client's logo, for use in user-facing UIs such as consent
pages and application pages.",
          "propertyOrder" : 25350,
          "items" : {
            "type" : "string"
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
```

```
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "array",
              "required" : false
            }
          }
        }
      }
    },
    "signEncOAuth2ClientConfig" : {
      "type" : "object",
      "title" : "Signing and Encryption",
      "propertyOrder" : 3,
      "properties" : {
        "publicKeyLocation" : {
          "title" : "Public key selector",
          "description" : "Select the public key for this client to come from either the jwks_uri,
 manual jwks or X509 field.",
          "propertyOrder" : 25700,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : true
            }
          }
        },
        "requestParameterEncryptedEncryptionAlgorithm" : {
          "title" : "Request parameter encryption method",
          "description" : "JWE enc algorithm for encrypting the request parameter.<br><br>AM supports
 the following token encryption algorithms:<ul><li><code>A128GCM</code>, <code>A192GCM</code>,
 and <code>A256GCM</code> - AES in Galois Counter Mode (GCM) authenticated encryption mode.</
li><li><code>A128CBC-HS256</code>, <code>A192CBC-HS384</code>, and <code>A256CBC-HS512</code> - AES
 encryption in CBC mode, with HMAC-SHA-2 for integrity.</li></ul>",
          "propertyOrder" : 27700,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : true
            }
          }
        },
        "idTokenEncryptionMethod" : {
          "title" : "ID Token Encryption Method",
          "description" : "Encryption method the ID Token for this client must be encrypted with.",
          "propertyOrder" : 24800,
```

```
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : true
            }
          }
        },
        "idTokenPublicEncryptionKey" : {
          "title" : "Client ID Token Public Encryption Key",
          "description" : "A Base64 encoded public key for encrypting ID Tokens.",
          "propertyOrder" : 24900,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "clientJwtPublicKey" : {
          "title" : "Client JWT Bearer Public Key",
          "description" : "A Base64 encoded X509 certificate, containing the public key, represented
as a UTF-8 PEM file, of the key pair for signing the Client Bearer JWT.",
          "propertyOrder" : 25400,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "jwksCacheTimeout" : {
          "title" : "JWKs URI content cache timeout in ms",
          "description" : "To avoid loading the JWKS URI content for every token encryption, the JWKS
content is cached. This timeout defines the maximum of time the JWKS URI content can be cached before
being refreshed.",
          "propertyOrder" : 24110,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
```

```
              "required" : true
            },
            "value" : {
              "type" : "integer",
              "required" : true
            }
          }
        },
        "userinfoEncryptedResponseAlg" : {
          "title" : "User info encrypted response algorithm",
          "description" : "JWE algorithm for encrypting UserInfo Responses. If both signing and
 encryption are requested, the response will be signed then encrypted, with the result being a Nested
 JWT. The default, if omitted, is that no encryption is performed.",
          "propertyOrder" : 27300,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "userinfoEncryptedResponseEncryptionAlgorithm" : {
          "title" : "User info encrypted response encryption algorithm",
          "description" : "JWE enc algorithm for encrypting UserInfo Responses. If userinfo encrypted
 response algorithm is specified, the default for this value is A128CBC-HS256. When user info
 encrypted response encryption is included, user info encrypted response algorithm MUST also be
 provided.<br><br>AM supports the following token encryption algorithms:<ul><li><code>A128GCM</code>,
 <code>A192GCM</code>, and <code>A256GCM</code> - AES in Galois Counter Mode (GCM) authenticated
 encryption mode.</li><li><code>A128CBC-HS256</code>, <code>A192CBC-HS384</code>, and <code>A256CBC-
HS512</code> - AES encryption in CBC mode, with HMAC-SHA-2 for integrity.</li></ul>",
          "propertyOrder" : 27400,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : true
            }
          }
        },
        "requestParameterEncryptedAlg" : {
          "title" : "Request parameter encryption algorithm",
          "description" : "JWE algorithm for encrypting the request parameter.",
          "propertyOrder" : 27600,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
```

```
            "required" : true
          },
          "value" : {
            "type" : "string",
            "required" : false
          }
        }
      },
      "jwksUri" : {
        "title" : "Json Web Key URI",
        "description" : "The uri that contains the client's public keys in Json Web Key format.",
        "propertyOrder" : 24100,
        "type" : "object",
        "exampleValue" : "https://{{jwks-www}}/oauth2/{{realm}}/connect/jwk_uri",
        "properties" : {
          "inherited" : {
            "type" : "boolean",
            "required" : true
          },
          "value" : {
            "type" : "string",
            "required" : false
          }
        }
      },
      "idTokenEncryptionAlgorithm" : {
        "title" : "ID Token Encryption Algorithm",
        "description" : "Algorithm the ID Token for this client must be encrypted with.",
        "propertyOrder" : 24700,
        "type" : "object",
        "exampleValue" : "",
        "properties" : {
          "inherited" : {
            "type" : "boolean",
            "required" : true
          },
          "value" : {
            "type" : "string",
            "required" : true
          }
        }
      },
      "tokenIntrospectionResponseFormat" : {
        "title" : "Token introspection response format",
        "description" : "The token introspection endpoint offers different output format. see
https://tools.ietf.org/html/draft-ietf-oauth-jwt-introspection-response-03",
        "propertyOrder" : 27800,
        "type" : "object",
        "exampleValue" : "",
        "properties" : {
          "inherited" : {
            "type" : "boolean",
            "required" : true
          },
          "value" : {
            "type" : "string",
            "required" : true
          }
        }
```

```
      },
      "tokenIntrospectionEncryptedResponseEncryptionAlgorithm" : {
        "title" : "Token introspection encrypted response encryption algorithm",
        "description" : "JWE 'enc' algorithm REQUIRED for encrypting token introspection responses.
Sets the algorithm that will be used to encrypt the Plaintext of a JWE when the chosen introspection
response format is 'signed then encrypted'.",
        "propertyOrder" : 27830,
        "type" : "object",
        "exampleValue" : "",
        "properties" : {
          "inherited" : {
            "type" : "boolean",
            "required" : true
          },
          "value" : {
            "type" : "string",
            "required" : true
          }
        }
      },
      "mTLSCertificateBoundAccessTokens" : {
        "title" : "Use Certificate-Bound Access Tokens",
        "description" : "Whether access tokens issued to this client should be bound to the X.509
certificate it uses to authenticate to the token endpoint. If enabled (and the provider supports it)
then an x5t#S256 confirmation key will be added to all access tokens with the SHA-256 hash of the
client's certificate.",
        "propertyOrder" : 25507,
        "type" : "object",
        "exampleValue" : "",
        "properties" : {
          "inherited" : {
            "type" : "boolean",
            "required" : true
          },
          "value" : {
            "type" : "boolean",
            "required" : true
          }
        }
      },
      "idTokenEncryptionEnabled" : {
        "title" : "Enable ID Token Encryption",
        "description" : "Select to enable ID token encryption.",
        "propertyOrder" : 24600,
        "type" : "object",
        "exampleValue" : "",
        "properties" : {
          "inherited" : {
            "type" : "boolean",
            "required" : true
          },
          "value" : {
            "type" : "boolean",
            "required" : true
          }
        }
      },
      "idTokenSignedResponseAlg" : {
        "title" : "ID Token Signing Algorithm",
```

```
          "description" : "Algorithm the ID Token for this client must be signed with.",
          "propertyOrder" : 24500,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : true
            }
          }
        },
        "requestParameterSignedAlg" : {
          "title" : "Request parameter signing algorithm",
          "description" : "JWS algorithm for signing the request parameter.",
          "propertyOrder" : 27500,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "jwkStoreCacheMissCacheTime" : {
          "title" : "JWKs URI content cache miss cache time",
          "description" : "To avoid loading the JWKS URI content for every token signature
verification, especially when the kid is not in the jwks content already cached, the JWKS content
will be cache for a minimum period of time. This cache miss cache time defines the minimum of time
the JWKS URI content is cache.",
          "propertyOrder" : 24120,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "integer",
              "required" : true
            }
          }
        },
        "mTLSSubjectDN" : {
          "title" : "mTLS Subject DN",
          "description" : "Expected Subject DN of certificate used for mTLS client certificate
authentication. Defaults to CN=&lt;client_id&gt;. Only applicable when using CA-signed
certificates.",
          "propertyOrder" : 25406,
          "type" : "object",
```

```
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "tokenIntrospectionEncryptedResponseAlg" : {
          "title" : "Token introspection response encryption algorithm",
          "description" : "JWE \"alg\" algorithm REQUIRED for encrypting introspection responses. Sets
the algorithm that will be used to encrypt the Content Encryption Key when the chosen introspection
response format is 'signed then encrypted'.",
          "propertyOrder" : 27820,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : true
            }
          }
        },
        "mTLSTrustedCert" : {
          "title" : "mTLS Self-Signed Certificate",
          "description" : "Self-signed PEM-encoded X.509 certificate for mTLS client certificate
authentication.",
          "propertyOrder" : 25405,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "jwkSet" : {
          "title" : "Json Web Key",
          "description" : "Raw JSON Web Key value containing the client's public keys.",
          "propertyOrder" : 24200,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
```

```
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "tokenIntrospectionSignedResponseAlg" : {
          "title" : "Token introspection response signing algorithm",
          "description" : "Algorithm used for signing the introspection JWT response.",
          "propertyOrder" : 27810,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : true
            }
          }
        },
        "userinfoResponseFormat" : {
          "title" : "User info response format.",
          "description" : "The user info endpoint offers different output format. See http://
openid.net/specs/openid-connect-core-1_0.html#UserInfoResponse",
          "propertyOrder" : 27100,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : true
            }
          }
        },
        "tokenEndpointAuthSigningAlgorithm" : {
          "title" : "Token Endpoint Authentication Signing Algorithm",
          "description" : "The JWS algorithm that MUST be used for signing the JWT used to
 authenticate the Client at the Token Endpointfor the private_key_jwt and client_secret_jwt
 authentication methods. All Token Requests using these authentication methods from this Client MUST
 be rejected, if the JWT is not signed with this algorithm.",
          "propertyOrder" : 24130,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : true
```

```
            }
          }
        },
        "userinfoSignedResponseAlg" : {
          "title" : "User info signed response algorithm",
          "description" : "JWS algorithm for signing UserInfo Responses. If this is specified, the
response will be JWT <a href=\"https://tools.ietf.org/html/rfc7519\">JWT</a> serialized, and signed
using JWS. The default, if omitted, is for the UserInfo Response to return the Claims as a UTF-8
encoded JSON object using the application/json content-type.",
          "propertyOrder" : 27200,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        }
      }
    },
    "coreOpenIDClientConfig" : {
      "type" : "object",
      "title" : "OpenID Connect",
      "propertyOrder" : 2,
      "properties" : {
        "postLogoutRedirectUri" : {
          "title" : "Post Logout Redirect URIs",
          "description" : "URIs that can be redirected to after the client logout process.",
          "propertyOrder" : 25000,
          "items" : {
            "type" : "string"
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "array",
              "required" : false
            }
          }
        },
        "defaultMaxAgeEnabled" : {
          "title" : "Default Max Age Enabled",
          "description" : "Whether or not the default max age is enforced.",
          "propertyOrder" : 25600,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
```

```
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : true
            }
          }
        },
        "jwtTokenLifetime" : {
          "title" : "OpenID Connect JWT Token Lifetime (seconds)",
          "description" : "The time in seconds a JWT is valid for. <i>NB</i> If this field is set to
zero, JWT Token Lifetime of the OAuth2 Provider is used instead of.",
          "propertyOrder" : 26100,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "integer",
              "required" : true
            }
          }
        },
        "claims" : {
          "title" : "Claim(s)",
          "description" : "List of claim name translations, which will override those specified for
the AS. Claims are values that are presented to the user to inform them what data is being made
available to the Client.<br><br>Claims may be entered as simple strings or pipe separated strings
representing the internal claim name, locale, and localized description; e.g. \"name|en|Your full
name\". Locale strings are in the format <code>language + \"_\" + country + \"_\" + variant</code>,
e.g. en, en_GB, en_US_WIN. If the locale and pipe is omitted, the description is displayed to all
users having undefined locales. e.g. \"name|Your full name\". <i>NB</i> If the description is also
omitted, nothing is displayed to all users, e.g. specifying \"name|\" would allow the claim \"name\"
to be used by the client, but would not display it to the user when it was requested.<p>If a value is
not given here, the value will be computed from the OAuth 2 Provider settings.</p>",
          "propertyOrder" : 23400,
          "items" : {
            "type" : "string"
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "array",
              "required" : false
            }
          }
        },
        "clientSessionUri" : {
          "title" : "Client Session URI",
          "description" : "This is the URI that will be used to check messages sent to the session
management endpoints. This URI must match the origin of the message",
```

```
          "propertyOrder" : 25200,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "defaultAcrValues" : {
          "title" : "Default ACR values",
          "description" : "Default requested Authentication Context Class Reference
 values.<br><br>Array of strings that specifies the default acr values that the OP is being requested
 to use for processing requests from this Client, with the values appearing in order of preference.
 The Authentication Context Class satisfied by the authentication performed is returned as the
 acr Claim Value in the issued ID Token. The acr Claim is requested as a Voluntary Claim by this
 parameter. The acr_values_supported discovery element contains a list of the acr values supported by
 this server. Values specified in the acr_values request parameter or an individual acr Claim request
 override these default values.",
          "propertyOrder" : 25650,
          "items" : {
            "type" : "string"
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "array",
              "required" : false
            }
          }
        },
        "defaultMaxAge" : {
          "title" : "Default Max Age",
          "description" : "Minimum value 1. Sets the maximum length of time in seconds a session
 may be active after the authorization service has succeeded before the user must actively re-
authenticate.",
          "propertyOrder" : 25500,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "integer",
              "required" : true
            }
          }
```

```
        }
      }
    },
    "coreUmaClientConfig" : {
      "type" : "object",
      "title" : "UMA",
      "propertyOrder" : 4,
      "properties" : {
        "claimsRedirectionUris" : {
          "title" : "Claims Redirection URIs",
          "description" : "Redirection URIs for returning to the client from UMA claims collection
 (not yet supported). If multiple URIs are registered, the client MUST specify the URI that the user
 should be redirected to following approval. May not contain a fragment (#).",
          "propertyOrder" : 23200,
          "items" : {
            "type" : "string"
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "array",
              "required" : false
            }
          }
        }
      }
    }
  }
}
```

delete

Usage:

```
am> delete OAuth2Clients --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action OAuth2Clients --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action OAuth2Clients --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action OAuth2Clients --realm Realm --actionName nextdescendents
```

query

Querying the agents of a specific type

Usage:

```
am> query OAuth2Clients --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read OAuth2Clients --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update OAuth2Clients --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "coreOAuth2ClientConfig" : {
      "type" : "object",
      "title" : "Core",
      "propertyOrder" : 0,
      "properties" : {
        "accessTokenLifetime" : {
          "title" : "Access Token Lifetime (seconds)",
          "description" : "The time in seconds an access token is valid for. <i>NB</i> If this field
 is set to zero, Access Token Lifetime of the OAuth2 Provider is used instead of.",
          "propertyOrder" : 26000,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "integer",
              "required" : true
            }
          }
        },
        "agentgroup" : {
          "title" : "Group",
          "description" : "Add the client to a group to allow inheritance of property values from the
 group. <br>Changing the group will update inherited property values. <br>Inherited property values
 are copied to the client.",
          "propertyOrder" : 100,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "clientName" : {
          "title" : "Client Name",
          "description" : "This value is a readable name for this client.",
          "propertyOrder" : 25300,
          "items" : {
            "type" : "string"
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
```

```
              "type" : "array",
              "required" : false
            }
          }
        },
        "userpassword" : {
          "title" : "Client secret",
          "description" : "Client secret. Used when the client authenticates to AM.",
          "propertyOrder" : 23000,
          "required" : true,
          "type" : "string",
          "format" : "password",
          "exampleValue" : ""
        },
        "authorizationCodeLifetime" : {
          "title" : "Authorization Code Lifetime (seconds)",
          "description" : "The time in seconds an authorization code is valid for. <i>NB</i> If this
 field is set to zero, Authorization Code Lifetime of the OAuth2 Provider is used instead of.",
          "propertyOrder" : 25800,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "integer",
              "required" : true
            }
          }
        },
        "loopbackInterfaceRedirection" : {
          "title" : "Allow wildcard ports in redirect URIs",
          "description" : "This flag indicates whether wildcards can be used for port numbers in
 redirect URIs. When this toggle is set to true and a wildcard is used the only allowed combinations
 of protocols and hosts are: http://127.0.0.1, https://127.0.0.1, http://[::1], https://[::1],
 http://localhost, https://localhost The wild cards are permitted only for the port values. For
 example - <code>http://localhost:80*</code>, <code>http://localhost:80?0/{path}</code>, <code>http://
localhost:80[8-9]0/{path}</code>",
          "propertyOrder" : 23150,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : false
            }
          }
        },
        "status" : {
          "title" : "Status",
          "description" : "Status of the agent configuration.",
          "propertyOrder" : 200,
          "type" : "object",
```

```
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : true
            }
          }
        },
        "clientType" : {
          "title" : "Client type",
          "description" : "Type of OAuth 2.0 client. Confidential clients can keep their password
secret, and are typically web apps or other server-based clients. Public clients run the risk
of exposing their password to a host or user agent, such as rich browser applications or desktop
clients.",
          "propertyOrder" : 23100,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : true
            }
          }
        },
        "refreshTokenLifetime" : {
          "title" : "Refresh Token Lifetime (seconds)",
          "description" : "The time in seconds a refresh token is valid for. <i>NB</i> If this field
is set to zero, Refresh Token Lifetime of the OAuth2 Provider is used instead. If this field is set
to -1, the token will never expire.",
          "propertyOrder" : 25900,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "integer",
              "required" : true
            }
          }
        },
        "scopes" : {
          "title" : "Scope(s)",
          "description" : "Scope(s). Scopes are strings that are presented to the user for approval
and included in tokens so that the protected resource may make decisions about what to give access
to.<br><br>Scopes may be entered as simple strings or pipe separated strings representing the
internal scope name, locale, and localized description; e.g. \"read|en|Permission to view email
messages in your account\". Locale strings are in the format <code>language + \"_\" + country + \"_
\" + variant</code>, e.g. en, en_GB, en_US_WIN. If the locale and pipe is omitted, the description
```

```
 is displayed to all users having undefined locales. e.g. \"read|Permission to view email messages in
 your account\". <i>NB</i> If the description is also omitted, nothing is displayed to all users, e.g.
 specifying \"read|\" would allow the scope \"read\" to be used by the client, but would not display
 it to the user when it was requested.",
          "propertyOrder" : 23300,
          "items" : {
            "type" : "string"
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "array",
              "required" : false
            }
          }
        },
        "redirectionUris" : {
          "title" : "Redirection URIs",
          "description" : "Redirection URIs (optional for confidential clients). Complete URIs or URIs
 consisting of protocol + authority + path are registered so that the OAuth 2.0 provider can trust
 that tokens are sent to trusted entities. If multiple URI's are registered, the client MUST specify
 the URI that the user should be redirected to following approval. May not contain a fragment (#).",
          "propertyOrder" : 23200,
          "items" : {
            "type" : "string"
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "array",
              "required" : false
            }
          }
        },
        "defaultScopes" : {
          "title" : "Default Scope(s)",
          "description" : "Default Scope(s). Scopes automatically given to tokens.<br><br>Default
 Scopes may be entered as simple strings or pipe separated strings representing the internal scope
 name, locale, and localized description; e.g. \"read|en|Permission to view email messages in your
 account\". Locale strings are in the format <code>language + \"_\" + country + \"_\" + variant</
code>, e.g. en, en_GB, en_US_WIN. If the locale and pipe is omitted, the description is displayed to
 all users having undefined locales. e.g. \"read|Permission to view email messages in your account
\". <i>NB</i> If the description is also omitted, nothing is displayed to all users, e.g. specifying
 \"read|\" would allow the scope \"read\" to be used by the client, but would not display it to the
 user when it was requested.",
          "propertyOrder" : 23700,
          "items" : {
            "type" : "string"
          },
```

```
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "array",
              "required" : false
            }
          }
        }
      }
    },
    "advancedOAuth2ClientConfig" : {
      "type" : "object",
      "title" : "Advanced",
      "propertyOrder" : 1,
      "properties" : {
        "isConsentImplied" : {
          "title" : "Implied consent",
          "description" : "When enabled, the resource owner will not be asked for consent during
authorization flows. The OAuth2 Provider must be configured to allow clients to skip consent.",
          "propertyOrder" : 26200,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : true
            }
          }
        },
        "subjectType" : {
          "title" : "Subject Type",
          "description" : "The subject type added to responses for this client. This value must be
included in \"Subject Type Supported\" in OAuth2Provider service setting.",
          "propertyOrder" : 24400,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : true
            }
          }
        },
        "contacts" : {
          "title" : "Contacts",
          "description" : "Email addresses of users who can administrate this client.",
```

```
          "propertyOrder" : 23900,
          "items" : {
            "type" : "string"
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "array",
              "required" : false
            }
          }
        },
        "mixUpMitigation" : {
          "title" : "OAuth 2.0 Mix-Up Mitigation enabled",
          "description" : "Enables OAuth 2.0 mix-up mitigation on the authorization server
 side.<br><br>Enable this setting only if this OAuth 2.0 client supports the <a href=\"https://
tools.ietf.org/html/draft-ietf-oauth-mix-up-mitigation-01\">OAuth 2.0 Mix-Up Mitigation draft</a>,
 otherwise AM will fail to validate access token requests received from this client.",
          "propertyOrder" : 26300,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : true
            }
          }
        },
        "policyUri" : {
          "title" : "Privacy Policy URI",
          "description" : "The URI for the client's privacy policy, for use in user-facing consent
 pages.",
          "propertyOrder" : 25375,
          "items" : {
            "type" : "string"
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "array",
              "required" : false
            }
          }
        },
        "name" : {
```

```
          "title" : "Display name",
          "description" : "A client name that may be relevant to the resource owner when considering
approval.<br><br>The name may be entered as a single string or as pipe separated strings for
locale and localized name; e.g. \"en|The ExampleCo Intranet\". Locale strings are in the format
<code>language + \"_\" + country + \"_\" + variant</code>, e.g. en, en_GB, en_US_WIN. If the locale
is omitted, the name is displayed to all users having undefined locales. e.g. \"The ExampleCo
Intranet\".",
          "propertyOrder" : 23500,
          "items" : {
            "type" : "string"
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "array",
              "required" : false
            }
          }
        },
        "grantTypes" : {
          "title" : "Grant Types",
          "description" : "The set of Grant Types (OAuth2 Flows) that are permitted to be used by this
client.<br><br>If no Grant Types (OAuth2 Flows) are configured then AUTHORIZATION_CODE flow would be
permitted by default.",
          "propertyOrder" : 23800,
          "items" : {
            "type" : "string"
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "array",
              "required" : true
            }
          }
        },
        "updateAccessToken" : {
          "title" : "Access Token",
          "description" : "The access token used to update the client.",
          "propertyOrder" : 25100,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
```

```
              "required" : false
            }
          }
        },
        "descriptions" : {
          "title" : "Display description",
          "description" : "A description of the client or other information that may be relevant
to the resource owner when considering approval.<br><br>The description may be entered as a single
string or as pipe separated strings for locale and localized name; e.g. \"en|The company intranet
is requesting the following access permission\". Locale strings are in the format <code>language
+ \"_\" + country + \"_\" + variant</code>, e.g. en, en_GB, en_US_WIN. If the locale is omitted,
the description is displayed to all users having undefined locales. e.g. \"The company intranet is
requesting the following access permission\".",
          "propertyOrder" : 23600,
          "items" : {
            "type" : "string"
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "array",
              "required" : false
            }
          }
        },
        "tokenEndpointAuthMethod" : {
          "title" : "Token Endpoint Authentication Method",
          "description" : "The authentication method with which a client authenticates to the
authorization server at the token endpoint. The authentication method applies to OIDC requests with
the openid scope.",
          "propertyOrder" : 24000,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : true
            }
          }
        },
        "responseTypes" : {
          "title" : "Response Types",
          "description" : "Response types this client will support and use.",
          "propertyOrder" : 23800,
          "items" : {
            "type" : "string"
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
```

```
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "array",
              "required" : true
            }
          }
        },
        "javascriptOrigins" : {
          "title" : "JavaScript Origins",
          "description" : "",
          "propertyOrder" : 23650,
          "items" : {
            "type" : "string"
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "array",
              "required" : false
            }
          }
        },
        "clientUri" : {
          "title" : "Client URI",
          "description" : "The URI for finding further information about the client from user-facing
UIs.",
          "propertyOrder" : 25325,
          "items" : {
            "type" : "string"
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "array",
              "required" : false
            }
          }
        },
        "sectorIdentifierUri" : {
          "title" : "Sector Identifier URI",
          "description" : "The Host component of this URL is used in the computation of pairwise
Subject Identifiers.",
          "propertyOrder" : 24300,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
```

```
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "requestUris" : {
          "title" : "Request uris",
          "description" : "Array of request_uri values that are pre-registered by the RP for use at
the OP.<br><br>The entire Request URI MUST NOT exceed 512 ASCII characters and MUST use either HTTP
or HTTPS. Otherwise the value will be ignored.",
          "propertyOrder" : 23700,
          "items" : {
            "type" : "string"
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "array",
              "required" : false
            }
          }
        },
        "logoUri" : {
          "title" : "Logo URI",
          "description" : "The URI for the client's logo, for use in user-facing UIs such as consent
pages and application pages.",
          "propertyOrder" : 25350,
          "items" : {
            "type" : "string"
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "array",
              "required" : false
            }
          }
        }
      }
    },
    "signEncOAuth2ClientConfig" : {
      "type" : "object",
      "title" : "Signing and Encryption",
      "propertyOrder" : 3,
```

```
      "properties" : {
        "publicKeyLocation" : {
          "title" : "Public key selector",
          "description" : "Select the public key for this client to come from either the jwks_uri,
 manual jwks or X509 field.",
          "propertyOrder" : 25700,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : true
            }
          }
        },
        "requestParameterEncryptedEncryptionAlgorithm" : {
          "title" : "Request parameter encryption method",
          "description" : "JWE enc algorithm for encrypting the request parameter.<br><br>AM supports
 the following token encryption algorithms:<ul><li><code>A128GCM</code>, <code>A192GCM</code>,
 and <code>A256GCM</code> - AES in Galois Counter Mode (GCM) authenticated encryption mode.</
li><li><code>A128CBC-HS256</code>, <code>A192CBC-HS384</code>, and <code>A256CBC-HS512</code> - AES
 encryption in CBC mode, with HMAC-SHA-2 for integrity.</li></ul>",
          "propertyOrder" : 27700,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : true
            }
          }
        },
        "idTokenEncryptionMethod" : {
          "title" : "ID Token Encryption Method",
          "description" : "Encryption method the ID Token for this client must be encrypted with.",
          "propertyOrder" : 24800,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : true
            }
          }
        },
        "idTokenPublicEncryptionKey" : {
          "title" : "Client ID Token Public Encryption Key",
```

```
          "description" : "A Base64 encoded public key for encrypting ID Tokens.",
          "propertyOrder" : 24900,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "clientJwtPublicKey" : {
          "title" : "Client JWT Bearer Public Key",
          "description" : "A Base64 encoded X509 certificate, containing the public key, represented
as a UTF-8 PEM file, of the key pair for signing the Client Bearer JWT.",
          "propertyOrder" : 25400,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "jwksCacheTimeout" : {
          "title" : "JWKs URI content cache timeout in ms",
          "description" : "To avoid loading the JWKS URI content for every token encryption, the JWKS
content is cached. This timeout defines the maximum of time the JWKS URI content can be cached before
being refreshed.",
          "propertyOrder" : 24110,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "integer",
              "required" : true
            }
          }
        },
        "userinfoEncryptedResponseAlg" : {
          "title" : "User info encrypted response algorithm",
          "description" : "JWE algorithm for encrypting UserInfo Responses. If both signing and
encryption are requested, the response will be signed then encrypted, with the result being a Nested
JWT. The default, if omitted, is that no encryption is performed.",
          "propertyOrder" : 27300,
          "type" : "object",
```

```
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "userinfoEncryptedResponseEncryptionAlgorithm" : {
          "title" : "User info encrypted response encryption algorithm",
          "description" : "JWE enc algorithm for encrypting UserInfo Responses. If userinfo encrypted
 response algorithm is specified, the default for this value is A128CBC-HS256. When user info
 encrypted response encryption is included, user info encrypted response algorithm MUST also be
 provided.<br><br>AM supports the following token encryption algorithms:<ul><li><code>A128GCM</code>,
 <code>A192GCM</code>, and <code>A256GCM</code> - AES in Galois Counter Mode (GCM) authenticated
 encryption mode.</li><li><code>A128CBC-HS256</code>, <code>A192CBC-HS384</code>, and <code>A256CBC-
HS512</code> - AES encryption in CBC mode, with HMAC-SHA-2 for integrity.</li></ul>",
          "propertyOrder" : 27400,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : true
            }
          }
        },
        "requestParameterEncryptedAlg" : {
          "title" : "Request parameter encryption algorithm",
          "description" : "JWE algorithm for encrypting the request parameter.",
          "propertyOrder" : 27600,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "jwksUri" : {
          "title" : "Json Web Key URI",
          "description" : "The uri that contains the client's public keys in Json Web Key format.",
          "propertyOrder" : 24100,
          "type" : "object",
          "exampleValue" : "https://{{jwks-www}}/oauth2/{{realm}}/connect/jwk_uri",
          "properties" : {
```

```
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "idTokenEncryptionAlgorithm" : {
          "title" : "ID Token Encryption Algorithm",
          "description" : "Algorithm the ID Token for this client must be encrypted with.",
          "propertyOrder" : 24700,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : true
            }
          }
        },
        "tokenIntrospectionResponseFormat" : {
          "title" : "Token introspection response format",
          "description" : "The token introspection endpoint offers different output format. see
https://tools.ietf.org/html/draft-ietf-oauth-jwt-introspection-response-03",
          "propertyOrder" : 27800,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : true
            }
          }
        },
        "tokenIntrospectionEncryptedResponseEncryptionAlgorithm" : {
          "title" : "Token introspection encrypted response encryption algorithm",
          "description" : "JWE 'enc' algorithm REQUIRED for encrypting token introspection responses.
Sets the algorithm that will be used to encrypt the Plaintext of a JWE when the chosen introspection
response format is 'signed then encrypted'.",
          "propertyOrder" : 27830,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
```

```
              "type" : "string",
              "required" : true
            }
          }
        },
        "mTLSCertificateBoundAccessTokens" : {
          "title" : "Use Certificate-Bound Access Tokens",
          "description" : "Whether access tokens issued to this client should be bound to the X.509
certificate it uses to authenticate to the token endpoint. If enabled (and the provider supports it)
then an x5t#S256 confirmation key will be added to all access tokens with the SHA-256 hash of the
client's certificate.",
          "propertyOrder" : 25507,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : true
            }
          }
        },
        "idTokenEncryptionEnabled" : {
          "title" : "Enable ID Token Encryption",
          "description" : "Select to enable ID token encryption.",
          "propertyOrder" : 24600,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : true
            }
          }
        },
        "idTokenSignedResponseAlg" : {
          "title" : "ID Token Signing Algorithm",
          "description" : "Algorithm the ID Token for this client must be signed with.",
          "propertyOrder" : 24500,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : true
            }
          }
        },
```

```
       "requestParameterSignedAlg" : {
         "title" : "Request parameter signing algorithm",
         "description" : "JWS algorithm for signing the request parameter.",
         "propertyOrder" : 27500,
         "type" : "object",
         "exampleValue" : "",
         "properties" : {
           "inherited" : {
             "type" : "boolean",
             "required" : true
           },
           "value" : {
             "type" : "string",
             "required" : false
           }
         }
       },
       "jwkStoreCacheMissCacheTime" : {
         "title" : "JWKs URI content cache miss cache time",
         "description" : "To avoid loading the JWKS URI content for every token signature
verification, especially when the kid is not in the jwks content already cached, the JWKS content
will be cache for a minimum period of time. This cache miss cache time defines the minimum of time
the JWKS URI content is cache.",
         "propertyOrder" : 24120,
         "type" : "object",
         "exampleValue" : "",
         "properties" : {
           "inherited" : {
             "type" : "boolean",
             "required" : true
           },
           "value" : {
             "type" : "integer",
             "required" : true
           }
         }
       },
       "mTLSSubjectDN" : {
         "title" : "mTLS Subject DN",
         "description" : "Expected Subject DN of certificate used for mTLS client certificate
authentication. Defaults to CN=&lt;client_id&gt;. Only applicable when using CA-signed
certificates.",
         "propertyOrder" : 25406,
         "type" : "object",
         "exampleValue" : "",
         "properties" : {
           "inherited" : {
             "type" : "boolean",
             "required" : true
           },
           "value" : {
             "type" : "string",
             "required" : false
           }
         }
       },
       "tokenIntrospectionEncryptedResponseAlg" : {
         "title" : "Token introspection response encryption algorithm",
```

```
          "description" : "JWE \"alg\" algorithm REQUIRED for encrypting introspection responses. Sets
the algorithm that will be used to encrypt the Content Encryption Key when the chosen introspection
response format is 'signed then encrypted'.",
          "propertyOrder" : 27820,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : true
            }
          }
        },
        "mTLSTrustedCert" : {
          "title" : "mTLS Self-Signed Certificate",
          "description" : "Self-signed PEM-encoded X.509 certificate for mTLS client certificate
authentication.",
          "propertyOrder" : 25405,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "jwkSet" : {
          "title" : "Json Web Key",
          "description" : "Raw JSON Web Key value containing the client's public keys.",
          "propertyOrder" : 24200,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "tokenIntrospectionSignedResponseAlg" : {
          "title" : "Token introspection response signing algorithm",
          "description" : "Algorithm used for signing the introspection JWT response.",
          "propertyOrder" : 27810,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
```

```
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : true
            }
          }
        },
        "userinfoResponseFormat" : {
          "title" : "User info response format.",
          "description" : "The user info endpoint offers different output format. See http://
openid.net/specs/openid-connect-core-1_0.html#UserInfoResponse",
          "propertyOrder" : 27100,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : true
            }
          }
        },
        "tokenEndpointAuthSigningAlgorithm" : {
          "title" : "Token Endpoint Authentication Signing Algorithm",
          "description" : "The JWS algorithm that MUST be used for signing the JWT used to
 authenticate the Client at the Token Endpointfor the private_key_jwt and client_secret_jwt
 authentication methods. All Token Requests using these authentication methods from this Client MUST
 be rejected, if the JWT is not signed with this algorithm.",
          "propertyOrder" : 24130,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : true
            }
          }
        },
        "userinfoSignedResponseAlg" : {
          "title" : "User info signed response algorithm",
          "description" : "JWS algorithm for signing UserInfo Responses. If this is specified, the
 response will be JWT <a href=\"https://tools.ietf.org/html/rfc7519\">JWT</a> serialized, and signed
 using JWS. The default, if omitted, is for the UserInfo Response to return the Claims as a UTF-8
 encoded JSON object using the application/json content-type.",
          "propertyOrder" : 27200,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
```

```
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        }
      }
    },
    "coreOpenIDClientConfig" : {
      "type" : "object",
      "title" : "OpenID Connect",
      "propertyOrder" : 2,
      "properties" : {
        "postLogoutRedirectUri" : {
          "title" : "Post Logout Redirect URIs",
          "description" : "URIs that can be redirected to after the client logout process.",
          "propertyOrder" : 25000,
          "items" : {
            "type" : "string"
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "array",
              "required" : false
            }
          }
        },
        "defaultMaxAgeEnabled" : {
          "title" : "Default Max Age Enabled",
          "description" : "Whether or not the default max age is enforced.",
          "propertyOrder" : 25600,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : true
            }
          }
        },
        "jwtTokenLifetime" : {
          "title" : "OpenID Connect JWT Token Lifetime (seconds)",
          "description" : "The time in seconds a JWT is valid for. <i>NB</i> If this field is set to
zero, JWT Token Lifetime of the OAuth2 Provider is used instead of.",
          "propertyOrder" : 26100,
          "type" : "object",
```

```
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "integer",
              "required" : true
            }
          }
        },
        "claims" : {
          "title" : "Claim(s)",
          "description" : "List of claim name translations, which will override those specified for
the AS. Claims are values that are presented to the user to inform them what data is being made
available to the Client.<br><br>Claims may be entered as simple strings or pipe separated strings
representing the internal claim name, locale, and localized description; e.g. \"name|en|Your full
name\". Locale strings are in the format <code>language + \"_\" + country + \"_\" + variant</code>,
e.g. en, en_GB, en_US_WIN. If the locale and pipe is omitted, the description is displayed to all
users having undefined locales. e.g. \"name|Your full name\". <i>NB</i> If the description is also
omitted, nothing is displayed to all users, e.g. specifying \"name|\" would allow the claim \"name\"
to be used by the client, but would not display it to the user when it was requested.<p>If a value is
not given here, the value will be computed from the OAuth 2 Provider settings.</p>",
          "propertyOrder" : 23400,
          "items" : {
            "type" : "string"
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "array",
              "required" : false
            }
          }
        },
        "clientSessionUri" : {
          "title" : "Client Session URI",
          "description" : "This is the URI that will be used to check messages sent to the session
management endpoints. This URI must match the origin of the message",
          "propertyOrder" : 25200,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
```

```
        "defaultAcrValues" : {
          "title" : "Default ACR values",
          "description" : "Default requested Authentication Context Class Reference
 values.<br><br>Array of strings that specifies the default acr values that the OP is being requested
 to use for processing requests from this Client, with the values appearing in order of preference.
 The Authentication Context Class satisfied by the authentication performed is returned as the
 acr Claim Value in the issued ID Token. The acr Claim is requested as a Voluntary Claim by this
 parameter. The acr_values_supported discovery element contains a list of the acr values supported by
 this server. Values specified in the acr_values request parameter or an individual acr Claim request
 override these default values.",
          "propertyOrder" : 25650,
          "items" : {
            "type" : "string"
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "array",
              "required" : false
            }
          }
        },
        "defaultMaxAge" : {
          "title" : "Default Max Age",
          "description" : "Minimum value 1. Sets the maximum length of time in seconds a session
 may be active after the authorization service has succeeded before the user must actively re-
authenticate.",
          "propertyOrder" : 25500,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "integer",
              "required" : true
            }
          }
        }
      }
    },
    "coreUmaClientConfig" : {
      "type" : "object",
      "title" : "UMA",
      "propertyOrder" : 4,
      "properties" : {
        "claimsRedirectionUris" : {
          "title" : "Claims Redirection URIs",
          "description" : "Redirection URIs for returning to the client from UMA claims collection
 (not yet supported). If multiple URIs are registered, the client MUST specify the URI that the user
 should be redirected to following approval. May not contain a fragment (#).",
          "propertyOrder" : 23200,
```

```
          "items" : {
            "type" : "string"
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "array",
              "required" : false
            }
          }
        }
      }
    }
  }
}
```

OAuth2Module

Realm Operations

Resource path: `/realm-config/authentication/modules/oauth2`

Resource version: `1.0`

create

Usage:

```
am> create OAuth2Module --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "smtpHostName" : {
      "title" : "SMTP host",
      "description" : "The mail host that will be used by the Email Gateway implementation",
```

```
      "propertyOrder" : 2300,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "clientId" : {
      "title" : "Client Id",
      "description" : "OAuth client_id parameter<br><br>For more information on the OAuth client_id
 parameter refer to the <a href=\"http://tools.ietf.org/html/rfc6749#section-2.3.1\" target=\"_blank
\">RFC 6749</a>, section 2.3.1",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "smtpFromAddress" : {
      "title" : "SMTP From address",
      "description" : "The email address on behalf of whom the messages will be sent",
      "propertyOrder" : 2800,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "accountProviderClass" : {
      "title" : "Account Provider",
      "description" : "Name of the class implementing the account provider.<br><br>This class
 is used by the module to find the account from the attributes mapped by the Account Mapper
 <code>org.forgerock.openam.authentication.modules.common.mapping.AccountProvider</code>
 interface.<br/>String constructor parameters can be provided by appending <code>|</code> separated
 values.",
      "propertyOrder" : 900,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "oauth2EmailAttribute" : {
      "title" : "Email attribute in OAuth2 Response",
      "description" : "Attribute from the OAuth2 response used to send activation code
 emails.<br><br>The attribute in the response from the profile service in the OAuth 2.0 Provider that
 contains the email address of the authenticated user. This address will be used to send an email with
 an activation code when the accounts are allowed to be created dynamically.",
      "propertyOrder" : 1500,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "promptForPassword" : {
      "title" : "Prompt for password setting and activation code",
      "description" : "Users must set a password and complete the activation flow during dynamic
 profile creation.<br><br>If this is enabled, the user must set a password before the system creates
 an account dynamically and an activation code will be sent to the user's email address. The account
 will be created only if the password and activation code are properly set. <br />If this is disabled,
 the account will be created transparently without prompting the user.",
      "propertyOrder" : 1700,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "smtpUsername" : {
```

```
      "title" : "SMTP User Name",
      "description" : "If the SMTP Service requires authentication, configure the user name here",
      "propertyOrder" : 2500,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "ssoProxyUrl" : {
      "title" : "Proxy URL",
      "description" : "The URL to the OpenAM OAuth proxy JSP<br><br>This URL should only be changed
 from the default, if an external server is performing the GET to POST proxying. The default is
 <code>/openam/oauth2c/OAuthProxy.jsp</code>",
      "propertyOrder" : 800,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "accessTokenEndpointUrl" : {
      "title" : "Access Token Endpoint URL",
      "description" : "OAuth access token endpoint URL<br><br>This is the URL endpoint for
 access token retrieval provided by the OAuth Identity Provider. Refer to the <a href=\"http://
tools.ietf.org/html/rfc6749#section-3.2\" target=\"_blank\">RFC 6749</a>, section 3.2",
      "propertyOrder" : 400,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "mixUpMitigation" : {
      "title" : "OAuth 2.0 Mix-Up Mitigation enabled",
      "description" : "Enables OAuth 2.0 mix-up mitigation<br><br>The authorization
 server must support the <a href=\"https://tools.ietf.org/html/draft-ietf-oauth-mix-up-
mitigation-01#section-3.1\">OAuth 2.0 Mix-Up Mitigation draft</a>, otherwise OpenAM will fail to
 validate responses from the authorization server. If only the OAuth 2.0 protocol is utilized, make
 sure that the accepted issuer value is set in the \"Token Issuer\" setting.",
      "propertyOrder" : 3300,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "accessTokenParameterName" : {
      "title" : "OAuth2 Access Token Profile Service Parameter name",
      "description" : "The name of the parameter that will contain the access token value when
 accessing the profile service",
      "propertyOrder" : 700,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "mapToAnonymousUser" : {
      "title" : "Map to anonymous user",
      "description" : "Enabled anonymous user access to OpenAM for OAuth authenticated users<br><br>If
 selected, the authenticated users in the OAuth 2.0 Provider will be mapped to the anonymous user
 configured in the next parameter.<br/>If not selected the users authenticated will be mapped by the
 parameters configured in the account mapper.<br/><br/><i>NB </i>If <i>Create account if it does not
 exist</i> is enabled, that parameter takes precedence.",
      "propertyOrder" : 1800,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
```

```
    },
    "accountMapperConfiguration" : {
      "title" : "Account Mapper Configuration",
      "description" : "Mapping of OAuth account to local OpenAM account<br><br>Attribute configuration
 that will be used to map the account of the user authenticated in the OAuth 2.0 Provider to the local
 data store in the OpenAM. Example: <code>OAuth2.0_attribute=local_attribute</code>",
      "propertyOrder" : 1100,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "mailGatewayClass" : {
      "title" : "Mail Server Gateway implementation class",
      "description" : "The class used by the module to send email.<br><br>This class is used by the
 module to send email. A custom implementation can be provided.<br/><br/>The custom implementation
 must implement the <code>org.forgerock.openam.authentication.modules.oauth2.EmailGateway</code>",
      "propertyOrder" : 2200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "authenticationEndpointUrl" : {
      "title" : "Authentication Endpoint URL",
      "description" : "OAuth authentication endpoint URL<br><br>This is the URL endpoint for OAuth
 authentication provided by the OAuth Identity Provider",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "authenticationLevel" : {
      "title" : "Authentication Level",
      "description" : "The authentication level associated with this module.<br><br>Each
 authentication module has an authentication level that can be used to indicate the level of security
 associated with the module; 0 is the lowest (and the default).",
      "propertyOrder" : 2900,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "openidConnectContextValue" : {
      "title" : "OpenID Connect validation configuration value",
      "description" : "Required when the 'openid' scope is included. The discovery url, or jwk
 url, or the client_secret, corresponding to the selection above.<br><br>If discovery or jwk url
 entered, entry must be in valid url format, <br/>e.g. https://accounts.google.com/.well-known/openid-
configuration<br/><i>NB </i>If client_secret entered, entry is ignored and the value of the Client
 Secret is used.",
      "propertyOrder" : 3100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "anonymousUserName" : {
      "title" : "Anonymous User",
      "description" : "Username of the OpenAM anonymous user<br><br>The username of the user that will
 represent the anonymous user. This user account must already exist in the realm.",
```

```
      "propertyOrder" : 1900,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "userProfileServiceUrl" : {
      "title" : "User Profile Service URL",
      "description" : "User profile information URL<br><br>This URL endpoint provides user profile
 information and is provided by the OAuth Identity Provider<br/><br/><i>NB </i>This URL should return
 JSON objects in response",
      "propertyOrder" : 500,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "smtpSslEnabled" : {
      "title" : "SMTP SSL Enabled",
      "description" : "Tick this option if the SMTP Server provides SSL",
      "propertyOrder" : 2700,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "logoutBehaviour" : {
      "title" : "Logout options",
      "description" : "Controls how Logout options will be presented to the user.<br><br>The OAuth
 module has the following logout options for the user:<br/><br/><ul><li>Prompt: Prompt the user to
 logout from the OAuth 2.0 Provider</li><li>Logout: Logout from the OAuth 2.0 Provider and do not
 prompt</li><li>Do not logout: Do not logout the user from the OAuth 2.0 Provider and do not prompt</
li></ul>",
      "propertyOrder" : 2100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "clientSecret" : {
      "title" : "Client Secret",
      "description" : "OAuth client_secret parameter<br><br>For more information on the OAuth
 client_secret parameter refer to the <a href=\"http://tools.ietf.org/html/rfc6749#section-2.3.1\"
 target=\"_blank\">RFC 6749</a>, section 2.3.1",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
      "format" : "password",
      "exampleValue" : ""
    },
    "openidConnectContextType" : {
      "title" : "OpenID Connect validation configuration type",
      "description" : "Required when the 'openid' scope is included. Please select either 1. the
 issuer discovery url, 2. the issuer jwk url, or 3. the client_secret.",
      "propertyOrder" : 3000,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "saveAttributesInSession" : {
      "title" : "Save attributes in the session",
      "description" : "If this option is enabled, the attributes configured in the attribute mapper
 will be saved into the OpenAM session",
```

```
      "propertyOrder" : 1400,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "scope" : {
      "title" : "Scope",
      "description" : "OAuth scope; list of user profile properties<br><br>According to the OAuth
 2.0 Authorization Framework, scope is a space-separated list of user profile attributes that the
 client application requires. The list depends on the permissions that the resource owner grants to
 the client application.<br/><br/> Some authorization servers use non-standard separators for scopes.
 For example, Facebook takes a comma-separated list.<br/><br/> Default: <code>email, read_stream</
code> (Facebook example)",
      "propertyOrder" : 600,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "accountMapperClass" : {
      "title" : "Account Mapper",
      "description" : "Name of the class implementing the attribute mapping for the account
 search.<br><br>This class is used by the module to map from the account information
 received from the OAuth Identity Provider into OpenAM.<br/><br/>The class must implement
 the <code>org.forgerock.openam.authentication.modules.common.mapping.AttributeMapper</code>
 interface.<br/>Provided implementations
 are:<ul><li>org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper</
li><li>org.forgerock.openam.authentication.modules.oidc.JwtAttributeMapper (can only be used when
 using the openid scope)</li></ul>String constructor parameters can be provided by appending <code>|</
code> separated values.",
      "propertyOrder" : 1000,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "attributeMapperConfiguration" : {
      "title" : "Attribute Mapper Configuration",
      "description" : "Mapping of OAuth attributes to local OpenAM attributes<br><br>Attribute
 configuration that will be used to map the user info obtained from the OAuth 2.0 Provider to the
 local user data store in the OpenAM.<br/><br/>Example: <code>OAuth2.0_attribute=local_attribute</
code>",
      "propertyOrder" : 1300,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "smtpHostPort" : {
      "title" : "SMTP port",
      "description" : "The TCP port that will be used by the SMTP gateway",
      "propertyOrder" : 2400,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "oauth2LogoutServiceUrl" : {
      "title" : "OAuth 2.0 Provider logout service",
```

```
      "description" : "The URL of the OAuth Identity Providers Logout service<br><br>OAuth 2.0
 Identity Providers can have a logout service. If this logout functionality is required then the URL
 of the Logout endpoint should configured here.",
      "propertyOrder" : 2000,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "smtpPassword" : {
      "title" : "SMTP User Password",
      "description" : "The Password of the SMTP User Name",
      "propertyOrder" : 2600,
      "required" : true,
      "type" : "string",
      "format" : "password",
      "exampleValue" : ""
    },
    "attributeMappingClasses" : {
      "title" : "Attribute Mapper",
      "description" : "Name of the class that implements the attribute mapping<br><br>This
 class maps the OAuth properties into OpenAM properties. A custom attribute
 mapper can be provided.<br/><br/>A custom attribute mapper must implement the
 <code>org.forgerock.openam.authentication.modules.common.mapping.AttributeMapper</code>
 interface.<br/>Provided implementations
 are:<ul><li>org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper</
li><li>org.forgerock.openam.authentication.modules.oidc.JwtAttributeMapper (can only be used when
 using the openid scope)</li></ul>String constructor parameters can be provided by appending <code>|</
code> separated values.",
      "propertyOrder" : 1200,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "openidConnectIssuer" : {
      "title" : "Token Issuer",
      "description" : "Required when the 'openid' scope is included. Value must match the iss field in
 issued ID Token<br/>e.g. accounts.google.com<br><br>The issuer value MUST be provided when OAuth 2.0
 Mix-Up Mitigation is enabled.",
      "propertyOrder" : 3200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "createAccount" : {
      "title" : "Create account if it does not exist",
      "description" : "If the OAuth2 account does not exist in the local OpenAM data store, an account
 will be created dynamically.<br><br>If this is enabled, the account mapper could create the account
 dynamically if there is no account mapped. Before creating the account, a dialog prompting for
 a password and asking for an activation code can be shown if the parameter \"Prompt for password
 setting and activation code\" is enabled.<br /><br />If this flag is not enabled, 3 alternative
 options exist:<br/><br/><ol><li>The accounts need to have a user profile in the OpenAM User Data
 Store</li><li>The user does not have a user profile and the \"Ignore Profile\" is set in the
 Authentication Service of the realm.</li><li>The account is mapped to an anonymous account (see
 parameter \"Map to anonymous user\" and \"Anonymous User\")</li></ol>",
      "propertyOrder" : 1600,
      "required" : true,
```

```
      "type" : "boolean",
      "exampleValue" : ""
    }
  }
}
```

delete

Usage:

```
am> delete OAuth2Module --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action OAuth2Module --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action OAuth2Module --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action OAuth2Module --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query OAuth2Module --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read OAuth2Module --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update OAuth2Module --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "smtpHostName" : {
      "title" : "SMTP host",
      "description" : "The mail host that will be used by the Email Gateway implementation",
      "propertyOrder" : 2300,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "clientId" : {
      "title" : "Client Id",
      "description" : "OAuth client_id parameter<br><br>For more information on the OAuth client_id
 parameter refer to the <a href=\"http://tools.ietf.org/html/rfc6749#section-2.3.1\" target=\"_blank
\">RFC 6749</a>, section 2.3.1",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
```

```
   },
   "smtpFromAddress" : {
     "title" : "SMTP From address",
     "description" : "The email address on behalf of whom the messages will be sent",
     "propertyOrder" : 2800,
     "required" : true,
     "type" : "string",
     "exampleValue" : ""
   },
   "accountProviderClass" : {
     "title" : "Account Provider",
     "description" : "Name of the class implementing the account provider.<br><br>This class
is used by the module to find the account from the attributes mapped by the Account Mapper
<code>org.forgerock.openam.authentication.modules.common.mapping.AccountProvider</code>
interface.<br/>String constructor parameters can be provided by appending <code>|</code> separated
values.",
     "propertyOrder" : 900,
     "required" : true,
     "type" : "string",
     "exampleValue" : ""
   },
   "oauth2EmailAttribute" : {
     "title" : "Email attribute in OAuth2 Response",
     "description" : "Attribute from the OAuth2 response used to send activation code
emails.<br><br>The attribute in the response from the profile service in the OAuth 2.0 Provider that
contains the email address of the authenticated user. This address will be used to send an email with
an activation code when the accounts are allowed to be created dynamically.",
     "propertyOrder" : 1500,
     "required" : true,
     "type" : "string",
     "exampleValue" : ""
   },
   "promptForPassword" : {
     "title" : "Prompt for password setting and activation code",
     "description" : "Users must set a password and complete the activation flow during dynamic
profile creation.<br><br>If this is enabled, the user must set a password before the system creates
an account dynamically and an activation code will be sent to the user's email address. The account
will be created only if the password and activation code are properly set. <br />If this is disabled,
the account will be created transparently without prompting the user.",
     "propertyOrder" : 1700,
     "required" : true,
     "type" : "boolean",
     "exampleValue" : ""
   },
   "smtpUsername" : {
     "title" : "SMTP User Name",
     "description" : "If the SMTP Service requires authentication, configure the user name here",
     "propertyOrder" : 2500,
     "required" : true,
     "type" : "string",
     "exampleValue" : ""
   },
   "ssoProxyUrl" : {
     "title" : "Proxy URL",
     "description" : "The URL to the OpenAM OAuth proxy JSP<br><br>This URL should only be changed
from the default, if an external server is performing the GET to POST proxying. The default is
<code>/openam/oauth2c/OAuthProxy.jsp</code>",
     "propertyOrder" : 800,
     "required" : true,
```

```
      "type" : "string",
      "exampleValue" : ""
    },
    "accessTokenEndpointUrl" : {
      "title" : "Access Token Endpoint URL",
      "description" : "OAuth access token endpoint URL<br><br>This is the URL endpoint for
 access token retrieval provided by the OAuth Identity Provider. Refer to the <a href=\"http://
tools.ietf.org/html/rfc6749#section-3.2\" target=\"_blank\">RFC 6749</a>, section 3.2",
      "propertyOrder" : 400,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "mixUpMitigation" : {
      "title" : "OAuth 2.0 Mix-Up Mitigation enabled",
      "description" : "Enables OAuth 2.0 mix-up mitigation<br><br>The authorization
 server must support the <a href=\"https://tools.ietf.org/html/draft-ietf-oauth-mix-up-
mitigation-01#section-3.1\">OAuth 2.0 Mix-Up Mitigation draft</a>, otherwise OpenAM will fail to
 validate responses from the authorization server. If only the OAuth 2.0 protocol is utilized, make
 sure that the accepted issuer value is set in the \"Token Issuer\" setting.",
      "propertyOrder" : 3300,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "accessTokenParameterName" : {
      "title" : "OAuth2 Access Token Profile Service Parameter name",
      "description" : "The name of the parameter that will contain the access token value when
 accessing the profile service",
      "propertyOrder" : 700,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "mapToAnonymousUser" : {
      "title" : "Map to anonymous user",
      "description" : "Enabled anonymous user access to OpenAM for OAuth authenticated users<br><br>If
 selected, the authenticated users in the OAuth 2.0 Provider will be mapped to the anonymous user
 configured in the next parameter.<br/>If not selected the users authenticated will be mapped by the
 parameters configured in the account mapper.<br/><br/><i>NB </i>If <i>Create account if it does not
 exist</i> is enabled, that parameter takes precedence.",
      "propertyOrder" : 1800,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "accountMapperConfiguration" : {
      "title" : "Account Mapper Configuration",
      "description" : "Mapping of OAuth account to local OpenAM account<br><br>Attribute configuration
 that will be used to map the account of the user authenticated in the OAuth 2.0 Provider to the local
 data store in the OpenAM. Example: <code>OAuth2.0_attribute=local_attribute</code>",
      "propertyOrder" : 1100,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
```

```
    "mailGatewayClass" : {
      "title" : "Mail Server Gateway implementation class",
      "description" : "The class used by the module to send email.<br><br>This class is used by the
 module to send email. A custom implementation can be provided.<br/><br/>The custom implementation
 must implement the <code>org.forgerock.openam.authentication.modules.oauth2.EmailGateway</code>",
      "propertyOrder" : 2200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "authenticationEndpointUrl" : {
      "title" : "Authentication Endpoint URL",
      "description" : "OAuth authentication endpoint URL<br><br>This is the URL endpoint for OAuth
 authentication provided by the OAuth Identity Provider",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "authenticationLevel" : {
      "title" : "Authentication Level",
      "description" : "The authentication level associated with this module.<br><br>Each
 authentication module has an authentication level that can be used to indicate the level of security
 associated with the module; 0 is the lowest (and the default).",
      "propertyOrder" : 2900,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "openidConnectContextValue" : {
      "title" : "OpenID Connect validation configuration value",
      "description" : "Required when the 'openid' scope is included. The discovery url, or jwk
 url, or the client_secret, corresponding to the selection above.<br><br>If discovery or jwk url
 entered, entry must be in valid url format, <br/>e.g. https://accounts.google.com/.well-known/openid-
configuration<br/><i>NB </i>If client_secret entered, entry is ignored and the value of the Client
 Secret is used.",
      "propertyOrder" : 3100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "anonymousUserName" : {
      "title" : "Anonymous User",
      "description" : "Username of the OpenAM anonymous user<br><br>The username of the user that will
 represent the anonymous user. This user account must already exist in the realm.",
      "propertyOrder" : 1900,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "userProfileServiceUrl" : {
      "title" : "User Profile Service URL",
      "description" : "User profile information URL<br><br>This URL endpoint provides user profile
 information and is provided by the OAuth Identity Provider<br/><br/><i>NB </i>This URL should return
 JSON objects in response",
      "propertyOrder" : 500,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
```

```
    },
    "smtpSslEnabled" : {
      "title" : "SMTP SSL Enabled",
      "description" : "Tick this option if the SMTP Server provides SSL",
      "propertyOrder" : 2700,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "logoutBehaviour" : {
      "title" : "Logout options",
      "description" : "Controls how Logout options will be presented to the user.<br><br>The OAuth
 module has the following logout options for the user:<br/><br/><ul><li>Prompt: Prompt the user to
 logout from the OAuth 2.0 Provider</li><li>Logout: Logout from the OAuth 2.0 Provider and do not
 prompt</li><li>Do not logout: Do not logout the user from the OAuth 2.0 Provider and do not prompt</
li></ul>",
      "propertyOrder" : 2100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "clientSecret" : {
      "title" : "Client Secret",
      "description" : "OAuth client_secret parameter<br><br>For more information on the OAuth
 client_secret parameter refer to the <a href=\"http://tools.ietf.org/html/rfc6749#section-2.3.1\"
 target=\"_blank\">RFC 6749</a>, section 2.3.1",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
      "format" : "password",
      "exampleValue" : ""
    },
    "openidConnectContextType" : {
      "title" : "OpenID Connect validation configuration type",
      "description" : "Required when the 'openid' scope is included. Please select either 1. the
 issuer discovery url, 2. the issuer jwk url, or 3. the client_secret.",
      "propertyOrder" : 3000,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "saveAttributesInSession" : {
      "title" : "Save attributes in the session",
      "description" : "If this option is enabled, the attributes configured in the attribute mapper
 will be saved into the OpenAM session",
      "propertyOrder" : 1400,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "scope" : {
      "title" : "Scope",
      "description" : "OAuth scope; list of user profile properties<br><br>According to the OAuth
 2.0 Authorization Framework, scope is a space-separated list of user profile attributes that the
 client application requires. The list depends on the permissions that the resource owner grants to
 the client application.<br/><br/> Some authorization servers use non-standard separators for scopes.
 For example, Facebook takes a comma-separated list.<br/><br/> Default: <code>email, read_stream</
code> (Facebook example)",
      "propertyOrder" : 600,
```

```
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "accountMapperClass" : {
      "title" : "Account Mapper",
      "description" : "Name of the class implementing the attribute mapping for the account
 search.<br><br>This class is used by the module to map from the account information
 received from the OAuth Identity Provider into OpenAM.<br/><br/>The class must implement
 the <code>org.forgerock.openam.authentication.modules.common.mapping.AttributeMapper</code>
 interface.<br/>Provided implementations
 are:<ul><li>org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper</
li><li>org.forgerock.openam.authentication.modules.oidc.JwtAttributeMapper (can only be used when
 using the openid scope)</li></ul>String constructor parameters can be provided by appending <code>|</
code> separated values.",
      "propertyOrder" : 1000,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "attributeMapperConfiguration" : {
      "title" : "Attribute Mapper Configuration",
      "description" : "Mapping of OAuth attributes to local OpenAM attributes<br><br>Attribute
 configuration that will be used to map the user info obtained from the OAuth 2.0 Provider to the
 local user data store in the OpenAM.<br/><br/>Example: <code>OAuth2.0_attribute=local_attribute</
code>",
      "propertyOrder" : 1300,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "smtpHostPort" : {
      "title" : "SMTP port",
      "description" : "The TCP port that will be used by the SMTP gateway",
      "propertyOrder" : 2400,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "oauth2LogoutServiceUrl" : {
      "title" : "OAuth 2.0 Provider logout service",
      "description" : "The URL of the OAuth Identity Providers Logout service<br><br>OAuth 2.0
 Identity Providers can have a logout service. If this logout functionality is required then the URL
 of the Logout endpoint should configured here.",
      "propertyOrder" : 2000,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "smtpPassword" : {
      "title" : "SMTP User Password",
      "description" : "The Password of the SMTP User Name",
      "propertyOrder" : 2600,
      "required" : true,
      "type" : "string",
      "format" : "password",
```

```
      "exampleValue" : ""
    },
    "attributeMappingClasses" : {
      "title" : "Attribute Mapper",
      "description" : "Name of the class that implements the attribute mapping<br><br>This
 class maps the OAuth properties into OpenAM properties. A custom attribute
 mapper can be provided.<br/><br/>A custom attribute mapper must implement the
 <code>org.forgerock.openam.authentication.modules.common.mapping.AttributeMapper</code>
 interface.<br/>Provided implementations
 are:<ul><li>org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper</
li><li>org.forgerock.openam.authentication.modules.oidc.JwtAttributeMapper (can only be used when
 using the openid scope)</li></ul>String constructor parameters can be provided by appending <code>|</
code> separated values.",
      "propertyOrder" : 1200,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "openidConnectIssuer" : {
      "title" : "Token Issuer",
      "description" : "Required when the 'openid' scope is included. Value must match the iss field in
 issued ID Token<br/>e.g. accounts.google.com<br><br>The issuer value MUST be provided when OAuth 2.0
 Mix-Up Mitigation is enabled.",
      "propertyOrder" : 3200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "createAccount" : {
      "title" : "Create account if it does not exist",
      "description" : "If the OAuth2 account does not exist in the local OpenAM data store, an account
 will be created dynamically.<br><br>If this is enabled, the account mapper could create the account
 dynamically if there is no account mapped. Before creating the account, a dialog prompting for
 a password and asking for an activation code can be shown if the parameter \"Prompt for password
 setting and activation code\" is enabled.<br /><br />If this flag is not enabled, 3 alternative
 options exist:<br/><br/><ol><li>The accounts need to have a user profile in the OpenAM User Data
 Store</li><li>The user does not have a user profile and the \"Ignore Profile\" is set in the
 Authentication Service of the realm.</li><li>The account is mapped to an anonymous account (see
 parameter \"Map to anonymous user\" and \"Anonymous User\")</li></ol>",
      "propertyOrder" : 1600,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    }
  }
}
```


Global Operations

Resource path: `/global-config/authentication/modules/oauth2`

Resource version: `1.0`

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action OAuth2Module --global --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action OAuth2Module --global --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action OAuth2Module --global --actionName nextdescendents
```

read

Usage:

```
am> read OAuth2Module --global
```

update

Usage:

```
am> update OAuth2Module --global --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "defaults" : {
      "properties" : {
        "oauth2EmailAttribute" : {
          "title" : "Email attribute in OAuth2 Response",
          "description" : "Attribute from the OAuth2 response used to send activation code
 emails.<br><br>The attribute in the response from the profile service in the OAuth 2.0 Provider that
```

```
 contains the email address of the authenticated user. This address will be used to send an email with
 an activation code when the accounts are allowed to be created dynamically.",
          "propertyOrder" : 1500,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "accessTokenParameterName" : {
          "title" : "OAuth2 Access Token Profile Service Parameter name",
          "description" : "The name of the parameter that will contain the access token value when
 accessing the profile service",
          "propertyOrder" : 700,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "userProfileServiceUrl" : {
          "title" : "User Profile Service URL",
          "description" : "User profile information URL<br><br>This URL endpoint provides user profile
 information and is provided by the OAuth Identity Provider<br/><br/><i>NB </i>This URL should return
 JSON objects in response",
          "propertyOrder" : 500,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "smtpSslEnabled" : {
          "title" : "SMTP SSL Enabled",
          "description" : "Tick this option if the SMTP Server provides SSL",
          "propertyOrder" : 2700,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "promptForPassword" : {
          "title" : "Prompt for password setting and activation code",
          "description" : "Users must set a password and complete the activation flow during dynamic
 profile creation.<br><br>If this is enabled, the user must set a password before the system creates
 an account dynamically and an activation code will be sent to the user's email address. The account
 will be created only if the password and activation code are properly set. <br />If this is disabled,
 the account will be created transparently without prompting the user.",
          "propertyOrder" : 1700,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "attributeMappingClasses" : {
          "title" : "Attribute Mapper",
          "description" : "Name of the class that implements the attribute
 mapping<br><br>This class maps the OAuth properties into OpenAM properties. A custom
 attribute mapper can be provided.<br/><br/>A custom attribute mapper must implement the
 <code>org.forgerock.openam.authentication.modules.common.mapping.AttributeMapper</code>
 interface.<br/>Provided implementations
 are:<ul><li>org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper</
li><li>org.forgerock.openam.authentication.modules.oidc.JwtAttributeMapper (can only be used when
 using the openid scope)</li></ul>String constructor parameters can be provided by appending <code>|</
code> separated values.",
          "propertyOrder" : 1200,
          "required" : true,
```

```
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "smtpFromAddress" : {
          "title" : "SMTP From address",
          "description" : "The email address on behalf of whom the messages will be sent",
          "propertyOrder" : 2800,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "ssoProxyUrl" : {
          "title" : "Proxy URL",
          "description" : "The URL to the OpenAM OAuth proxy JSP<br><br>This URL should only be
 changed from the default, if an external server is performing the GET to POST proxying. The default
 is <code>/openam/oauth2c/OAuthProxy.jsp</code>",
          "propertyOrder" : 800,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "authenticationLevel" : {
          "title" : "Authentication Level",
          "description" : "The authentication level associated with this module.<br><br>Each
 authentication module has an authentication level that can be used to indicate the level of security
 associated with the module; 0 is the lowest (and the default).",
          "propertyOrder" : 2900,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "logoutBehaviour" : {
          "title" : "Logout options",
          "description" : "Controls how Logout options will be presented to the user.<br><br>The OAuth
 module has the following logout options for the user:<br/><br/><ul><li>Prompt: Prompt the user to
 logout from the OAuth 2.0 Provider</li><li>Logout: Logout from the OAuth 2.0 Provider and do not
 prompt</li><li>Do not logout: Do not logout the user from the OAuth 2.0 Provider and do not prompt</
li></ul>",
          "propertyOrder" : 2100,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "anonymousUserName" : {
          "title" : "Anonymous User",
          "description" : "Username of the OpenAM anonymous user<br><br>The username of the user that
 will represent the anonymous user. This user account must already exist in the realm.",
          "propertyOrder" : 1900,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "mapToAnonymousUser" : {
          "title" : "Map to anonymous user",
          "description" : "Enabled anonymous user access to OpenAM for OAuth authenticated
 users<br><br>If selected, the authenticated users in the OAuth 2.0 Provider will be mapped to the
```

```
 anonymous user configured in the next parameter.<br/>If not selected the users authenticated will be
 mapped by the parameters configured in the account mapper.<br/><br/><i>NB </i>If <i>Create account if
 it does not exist</i> is enabled, that parameter takes precedence.",
          "propertyOrder" : 1800,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "saveAttributesInSession" : {
          "title" : "Save attributes in the session",
          "description" : "If this option is enabled, the attributes configured in the attribute
 mapper will be saved into the OpenAM session",
          "propertyOrder" : 1400,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "authenticationEndpointUrl" : {
          "title" : "Authentication Endpoint URL",
          "description" : "OAuth authentication endpoint URL<br><br>This is the URL endpoint for OAuth
 authentication provided by the OAuth Identity Provider",
          "propertyOrder" : 300,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "mailGatewayClass" : {
          "title" : "Mail Server Gateway implementation class",
          "description" : "The class used by the module to send email.<br><br>This class is used by
 the module to send email. A custom implementation can be provided.<br/><br/>The custom implementation
 must implement the <code>org.forgerock.openam.authentication.modules.oauth2.EmailGateway</code>",
          "propertyOrder" : 2200,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "openidConnectContextValue" : {
          "title" : "OpenID Connect validation configuration value",
          "description" : "Required when the 'openid' scope is included. The discovery url, or jwk
 url, or the client_secret, corresponding to the selection above.<br><br>If discovery or jwk url
 entered, entry must be in valid url format, <br/>e.g. https://accounts.google.com/.well-known/openid-
configuration<br/><i>NB </i>If client_secret entered, entry is ignored and the value of the Client
 Secret is used.",
          "propertyOrder" : 3100,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "smtpHostName" : {
          "title" : "SMTP host",
          "description" : "The mail host that will be used by the Email Gateway implementation",
          "propertyOrder" : 2300,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "scope" : {
          "title" : "Scope",
```

```
          "description" : "OAuth scope; list of user profile properties<br><br>According to the OAuth
 2.0 Authorization Framework, scope is a space-separated list of user profile attributes that the
 client application requires. The list depends on the permissions that the resource owner grants to
 the client application.<br/><br/> Some authorization servers use non-standard separators for scopes.
 For example, Facebook takes a comma-separated list.<br/><br/> Default: <code>email, read_stream</
code> (Facebook example)",
          "propertyOrder" : 600,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "smtpPassword" : {
          "title" : "SMTP User Password",
          "description" : "The Password of the SMTP User Name",
          "propertyOrder" : 2600,
          "required" : true,
          "type" : "string",
          "format" : "password",
          "exampleValue" : ""
        },
        "accessTokenEndpointUrl" : {
          "title" : "Access Token Endpoint URL",
          "description" : "OAuth access token endpoint URL<br><br>This is the URL endpoint for
 access token retrieval provided by the OAuth Identity Provider. Refer to the <a href=\"http://
tools.ietf.org/html/rfc6749#section-3.2\" target=\"_blank\">RFC 6749</a>, section 3.2",
          "propertyOrder" : 400,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "createAccount" : {
          "title" : "Create account if it does not exist",
          "description" : "If the OAuth2 account does not exist in the local OpenAM data store, an
 account will be created dynamically.<br><br>If this is enabled, the account mapper could create
 the account dynamically if there is no account mapped. Before creating the account, a dialog
 prompting for a password and asking for an activation code can be shown if the parameter \"Prompt
 for password setting and activation code\" is enabled.<br /><br />If this flag is not enabled, 3
 alternative options exist:<br/><br/><ol><li>The accounts need to have a user profile in the OpenAM
 User Data Store</li><li>The user does not have a user profile and the \"Ignore Profile\" is set in
 the Authentication Service of the realm.</li><li>The account is mapped to an anonymous account (see
 parameter \"Map to anonymous user\" and \"Anonymous User\")</li></ol>",
          "propertyOrder" : 1600,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "accountMapperClass" : {
          "title" : "Account Mapper",
          "description" : "Name of the class implementing the attribute mapping for the
 account search.<br><br>This class is used by the module to map from the account information
 received from the OAuth Identity Provider into OpenAM.<br/><br/>The class must implement
 the <code>org.forgerock.openam.authentication.modules.common.mapping.AttributeMapper</code>
 interface.<br/>Provided implementations
 are:<ul><li>org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper</
li><li>org.forgerock.openam.authentication.modules.oidc.JwtAttributeMapper (can only be used when
 using the openid scope)</li></ul>String constructor parameters can be provided by appending <code>|</
code> separated values.",
          "propertyOrder" : 1000,
          "required" : true,
```

```
          "type" : "string",
          "exampleValue" : ""
        },
        "accountProviderClass" : {
          "title" : "Account Provider",
          "description" : "Name of the class implementing the account provider.<br><br>This
 class is used by the module to find the account from the attributes mapped by the Account
 Mapper <code>org.forgerock.openam.authentication.modules.common.mapping.AccountProvider</code>
 interface.<br/>String constructor parameters can be provided by appending <code>|</code> separated
 values.",
          "propertyOrder" : 900,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "clientSecret" : {
          "title" : "Client Secret",
          "description" : "OAuth client_secret parameter<br><br>For more information on the OAuth
 client_secret parameter refer to the <a href=\"http://tools.ietf.org/html/rfc6749#section-2.3.1\"
 target=\"_blank\">RFC 6749</a>, section 2.3.1",
          "propertyOrder" : 200,
          "required" : true,
          "type" : "string",
          "format" : "password",
          "exampleValue" : ""
        },
        "openidConnectIssuer" : {
          "title" : "Token Issuer",
          "description" : "Required when the 'openid' scope is included. Value must match the iss
 field in issued ID Token<br/>e.g. accounts.google.com<br><br>The issuer value MUST be provided when
 OAuth 2.0 Mix-Up Mitigation is enabled.",
          "propertyOrder" : 3200,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "openidConnectContextType" : {
          "title" : "OpenID Connect validation configuration type",
          "description" : "Required when the 'openid' scope is included. Please select either 1. the
 issuer discovery url, 2. the issuer jwk url, or 3. the client_secret.",
          "propertyOrder" : 3000,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "mixUpMitigation" : {
          "title" : "OAuth 2.0 Mix-Up Mitigation enabled",
          "description" : "Enables OAuth 2.0 mix-up mitigation<br><br>The authorization
 server must support the <a href=\"https://tools.ietf.org/html/draft-ietf-oauth-mix-up-
mitigation-01#section-3.1\">OAuth 2.0 Mix-Up Mitigation draft</a>, otherwise OpenAM will fail to
 validate responses from the authorization server. If only the OAuth 2.0 protocol is utilized, make
 sure that the accepted issuer value is set in the \"Token Issuer\" setting.",
          "propertyOrder" : 3300,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "attributeMapperConfiguration" : {
          "title" : "Attribute Mapper Configuration",
```

```
          "description" : "Mapping of OAuth attributes to local OpenAM attributes<br><br>Attribute
 configuration that will be used to map the user info obtained from the OAuth 2.0 Provider to the
 local user data store in the OpenAM.<br/><br/>Example: <code>OAuth2.0_attribute=local_attribute</
code>",
          "propertyOrder" : 1300,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "smtpHostPort" : {
          "title" : "SMTP port",
          "description" : "The TCP port that will be used by the SMTP gateway",
          "propertyOrder" : 2400,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "oauth2LogoutServiceUrl" : {
          "title" : "OAuth 2.0 Provider logout service",
          "description" : "The URL of the OAuth Identity Providers Logout service<br><br>OAuth 2.0
 Identity Providers can have a logout service. If this logout functionality is required then the URL
 of the Logout endpoint should configured here.",
          "propertyOrder" : 2000,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "accountMapperConfiguration" : {
          "title" : "Account Mapper Configuration",
          "description" : "Mapping of OAuth account to local OpenAM account<br><br>Attribute
 configuration that will be used to map the account of the user authenticated in the OAuth 2.0
 Provider to the local data store in the OpenAM. Example: <code>OAuth2.0_attribute=local_attribute</
code>",
          "propertyOrder" : 1100,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "clientId" : {
          "title" : "Client Id",
          "description" : "OAuth client_id parameter<br><br>For more information on the OAuth
 client_id parameter refer to the <a href=\"http://tools.ietf.org/html/rfc6749#section-2.3.1\" target=
\"_blank\">RFC 6749</a>, section 2.3.1",
          "propertyOrder" : 100,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "smtpUsername" : {
          "title" : "SMTP User Name",
          "description" : "If the SMTP Service requires authentication, configure the user name here",
          "propertyOrder" : 2500,
          "required" : true,
```

```
          "type" : "string",
          "exampleValue" : ""
        }
      },
      "type" : "object",
      "title" : "Realm Defaults"
    }
  }
}
```

OAuth2Provider

Realm Operations

Resource path: `/realm-config/services/oauth-oidc`

Resource version: `1.0`

create

Usage:

```
am> create OAuth2Provider --realm Realm --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "advancedOAuth2Config" : {
      "type" : "object",
      "title" : "Advanced",
      "propertyOrder" : 1,
      "properties" : {
        "tlsCertificateRevocationCheckingEnabled" : {
          "title" : "Check TLS Certificate Revocation Status",
          "description" : "Whether to check if TLS client certificates have been revoked.<br><br>If
 enabled then AM will check if TLS client certificates used for client authentication have been
 revoked using either OCSP (preferred) or CRL. AM implements \"soft fail\" semantics: if the
 revocation status cannot be established due to a temporary error (e.g., network error) then the
 certificate is assumed to still be valid.",
          "propertyOrder" : 615,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "tlsOcspResponderUri" : {
```

```
          "title" : "OCSP Responder URI",
          "description" : "URI of the OCSP responder service to use for checking certificate
 revocation status.<br><br>If specified this value overrides any OCSP or CRL mechanisms specified in
 individual certificates.",
          "propertyOrder" : 616,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "tlsClientCertificateTrustedHeader" : {
          "title" : "Trusted TLS Client Certificate Header",
          "description" : "HTTP Header to receive TLS client certificates when TLS is terminated at a
 proxy.<br><br>Leave blank if not terminating TLS at a proxy. Ensure that the proxy is configured to
 strip this headerfrom incoming requests. Best practice is to use a random string.",
          "propertyOrder" : 600,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "tlsOcspResponderCert" : {
          "title" : "OCSP Responder Certificate",
          "description" : "PEM-encoded certificate to use to verify OCSP responses.<br><br>If
 specified this certificate will be used to verify the signature on all OCSP responses. Otherwise the
 appropriate certificate will be determined from the trusted CA certificates.",
          "propertyOrder" : 617,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "codeVerifierEnforced" : {
          "title" : "Code Verifier Parameter Required",
          "description" : "If enabled, requests using the authorization code grant require a
 <code>code_challenge</code> attribute.<br><br>For more information, read the <a href=\"https://
tools.ietf.org/html/rfc7636\">specification for this feature</a>.",
          "propertyOrder" : 270,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "tokenEncryptionEnabled" : {
          "title" : "Encrypt Client-Based Tokens",
          "description" : "Whether client-based access and refresh tokens should be
 encrypted.<br><br>Enabling token encryption will disable token signing as encryption is performed
 using direct symmetric encryption.",
          "propertyOrder" : 242,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "passwordGrantAuthService" : {
          "title" : "Password Grant Authentication Service",
          "description" : "The authentication service (chain or tree) that will be used to
 authenticate the username and password for the resource owner password credentials grant type.",
          "propertyOrder" : 430,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "tlsClientCertificateHeaderFormat" : {
```

```
          "title" : "TLS Client Certificate Header Format",
          "description" : "Format of the HTTP header used to communicate a client certificate
 from a reverse proxy.<br><br>The following formats are supported:<ul><li><code>URLENCODED_PEM</
code> - a URL-encoded PEM format certificate. This is the format used by Nginx.</
li><li><code>X_FORWARDED_CLIENT_CERT</code> - the <a target=\"_blank\" href=\"https://
www.envoyproxy.io/docs/envoy/latest/configuration/http/http_conn_man/headers#config-http-conn-man-
headers-x-forwarded-client-cert\">X-Forwarded-Client-Cert</a>format used by Envoy and Istio.</li></
ul>",
          "propertyOrder" : 605,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "displayNameAttribute" : {
          "title" : "User Display Name attribute",
          "description" : "The profile attribute that contains the name to be displayed for the user
 on the consent page.",
          "propertyOrder" : 120,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "createdTimestampAttribute" : {
          "title" : "Created Timestamp Attribute Name",
          "description" : "The identity Data Store attribute used to return created timestamp
 values.",
          "propertyOrder" : 350,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "supportedScopes" : {
          "title" : "Client Registration Scope Whitelist",
          "description" : "The set of scopes allowed when registering clients dynamically,
 with translations.<br><br><p>Scopes may be entered as simple strings or pipe-separated strings
 representing the internal scope name, locale, and localized description.</p><p>For example:
 <code>read|en|Permission to view email messages in your account</code></p><p>Locale strings are in
 the format: <code>language_country_variant</code>, for example <code>en</code>, <code>en_GB</code>,
 or <code>en_US_WIN</code>.</p><p>If the locale and pipe is omitted, the description is displayed
 to all users that have undefined locales.</p><p>If the description is also omitted, nothing is
 displayed on the consent page for the scope. For example specifying <code>read|</code> would allow
 the scope read to be used by the client, but would not display it to the user on the consent page
 when requested.</p>",
          "propertyOrder" : 130,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "allowedAudienceValues" : {
          "title" : "Additional Audience Values",
          "description" : "The additional audience values that will be permitted when verifying Client
 Authentication JWTs.<br><br>These audience values will be in addition to the AS base, issuer and
 endpoint URIs.",
          "propertyOrder" : 91,
          "required" : false,
          "items" : {
```

```
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "modifiedTimestampAttribute" : {
          "title" : "Modified Timestamp Attribute Name",
          "description" : "The identity Data Store attribute used to return modified timestamp
 values.<p>This attribute is paired together with the <em>Created Timestamp Attribute Name</em>
 attribute (<code>createdTimestampAttribute</code>). You can leave both attributes unset (default) or
 set them both. If you set only one attribute and leave the other blank, the access token fails with
 a 500 error.<p>For example, when you configure AM as an OpenID Connect Provider in a Mobile Connect
 application and use DS as an identity data store, the client accesses the <code>userinfo</code>
 endpoint to obtain the <code>updated_at</code> claim value in the ID token. The <code>updated_at</
code> claim obtains its value from the <code>modifiedTimestampAttribute</code> attribute in the
 user profile. If the profile has never been modified the <code>updated_at</code> claim uses the
 <code>createdTimestampAttribute</code> attribute. ",
          "propertyOrder" : 340,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "responseTypeClasses" : {
          "title" : "Response Type Plugins",
          "description" : "List of plugins that handle the valid <code>response_type</code>
 values.<br><br>OAuth 2.0 clients pass response types as parameters to the OAuth 2.0 Authorization
 endpoint (<code>/oauth2/authorize</code>) to indicate which grant type is requested from the
 provider. For example, the client passes <code>code</code> when requesting an authorization code,
 and <code>token</code> when requesting an access token.<p><p>Values in this list take the form
 <code>response-type|plugin-class-name</code>.",
          "propertyOrder" : 90,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "customLoginUrlTemplate" : {
          "title" : "Custom Login URL Template",
          "description" : "Custom URL for handling login, to override the default OpenAM login
 page.<br><br>Supports Freemarker syntax, with the following variables:<table><tr><th>Variable</
th><th>Description</th></tr><tr><td><code>gotoUrl</code></td><td><p>The URL to redirect to after
 login.</p></td></tr><tr><td><code>acrValues</code></td><td><p>The Authentication Context Class
 Reference (acr) values for the authorization request.</p></td></tr><tr><td><code>realm</code></
td><td><p>The OpenAM realm the authorization request was made on.</p></td></tr><tr><td><code>module</
code></td><td><p>The name of the OpenAM authentication module requested to perform resource
 owner authentication.</p></td></tr><tr><td><code>service</code></td><td><p>The name of the
 OpenAM authentication chain requested to perform resource owner authentication.</p></td></
tr><tr><td><code>locale</code></td><td><p>A space-separated list of locales, ordered by
 preference.</p></td></tr></table>The following example template redirects users to a non-OpenAM
 front end to handle login, which will then redirect back to the <code>/oauth2/authorize</code>
 endpoint with any required parameters:<p> <code>http://mylogin.com/login?goto=${goto}&lt;#if
 acrValues??&gt;&amp;acr_values=${acrValues}&lt;&#x2F;#if&gt;&lt;#if realm??&gt;&amp;realm=
${realm}&lt;&#x2F;#if&gt;&lt;#if module??&gt;&amp;module=${module}&lt;&#x2F;#if&gt;&lt;#if
 service??&gt;&amp;service=${service}&lt;&#x2F;#if&gt;&lt;#if locale??&gt;&amp;locale=
${locale}&lt;&#x2F;#if&gt;</code><br><b>NOTE</b>: Default OpenAM login page is constructed using
 \"Base URL Source\" service.",
          "propertyOrder" : 60,
```

```
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "moduleMessageEnabledInPasswordGrant" : {
          "title" : "Enable Auth Module Messages for Password Credentials Grant",
          "description" : "If enabled, authentication module failure messages are used to create
 Resource Owner Password Credentials Grant failure messages. If disabled, a standard authentication
 failed message is used.<br><br>The Password Grant Type requires the <code>grant_type=password</code>
 parameter.",
          "propertyOrder" : 440,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "hashSalt" : {
          "title" : "Subject Identifier Hash Salt",
          "description" : "If <i>pairwise</i> subject types are supported, it is <em>STRONGLY
 RECOMMENDED</em> to change this value. It is used in the salting of hashes for returning
 specific <code>sub</code> claims to individuals using the same <code>request_uri</code> or
 <code>sector_identifier_uri</code>.",
          "propertyOrder" : 260,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "supportedSubjectTypes" : {
          "title" : "Subject Types supported",
          "description" : "List of subject types supported. Valid values are:<ul><li><code>public</
code> - Each client receives the same subject (<code>sub</code>) value.</li><li><code>pairwise</code>
 - Each client receives a different subject (<code>sub</code>) value, to prevent correlation between
 clients.</li></ul>",
          "propertyOrder" : 150,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "scopeImplementationClass" : {
          "title" : "Scope Implementation Class",
          "description" : "The class that contains the required scope implementation, must implement
 the <code>org.forgerock.oauth2.core.ScopeValidator</code> interface.",
          "propertyOrder" : 70,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "tokenCompressionEnabled" : {
          "title" : "Client-Based Token Compression",
          "description" : "Whether client-based access and refresh tokens should be compressed.",
          "propertyOrder" : 223,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "grantTypes" : {
          "title" : "Grant Types",
```

```
          "description" : "The set of Grant Types (OAuth2 Flows) that are permitted to be used by this
 client.<br><br>If no Grant Types (OAuth2 Flows) are configured nothing will be permitted.",
          "propertyOrder" : 560,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "macaroonTokenFormat" : {
          "title" : "Macaroon Token Format",
          "description" : "The format to use when serializing and parsing Macaroons. V1 is bulky and
 should only be used when compatibility with older Macaroon libraries is required.",
          "propertyOrder" : 620,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "authenticationAttributes" : {
          "title" : "User Profile Attribute(s) the Resource Owner is Authenticated On",
          "description" : "Names of profile attributes that resource owners use to log in. You can add
 others to the default, for example <code>mail</code>.",
          "propertyOrder" : 100,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "tokenSigningAlgorithm" : {
          "title" : "OAuth2 Token Signing Algorithm",
          "description" : "Algorithm used to sign client-based OAuth 2.0 tokens in order to detect
 tampering.<br><br>OpenAM supports signing algorithms listed in JSON Web Algorithms (JWA): <a href=
\"https://tools.ietf.org/html/rfc7518#section-3.1\">\"alg\" (Algorithm) Header Parameter Values for
 JWS</a>:<ul><li><code>HS256</code> - HMAC with SHA-256.</li><li><code>HS384</code> - HMAC with
 SHA-384.</li><li><code>HS512</code> - HMAC with SHA-512.</li><li><code>ES256</code> - ECDSA with
 SHA-256 and NIST standard P-256 elliptic curve.</li><li><code>ES384</code> - ECDSA with SHA-384 and
 NIST standard P-384 elliptic curve.</li><li><code>ES512</code> - ECDSA with SHA-512 and NIST standard
 P-521 elliptic curve.</li><li><code>RS256</code> - RSASSA-PKCS-v1_5 using SHA-256.</li></ul>",
          "propertyOrder" : 220,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "defaultScopes" : {
          "title" : "Default Client Scopes",
          "description" : "List of scopes a client will be granted if they request registration
 without specifying which scopes they want. Default scopes are NOT auto-granted to clients created
 through the OpenAM console.",
          "propertyOrder" : 200,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
```

```
        "tlsCertificateBoundAccessTokensEnabled" : {
          "title" : "Support TLS Certificate-Bound Access Tokens",
          "description" : "Whether to bind access tokens to the client certificate when using TLS
 client certificate authentication.",
          "propertyOrder" : 610,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        }
      }
    },
    "consent" : {
      "type" : "object",
      "title" : "Consent",
      "propertyOrder" : 6,
      "properties" : {
        "supportedRcsRequestEncryptionAlgorithms" : {
          "title" : "Remote Consent Service Request Encryption Algorithms Supported",
          "description" : "Encryption algorithms supported to encrypt Remote Consent Service
 requests.<br><br>OpenAM supports the following encryption algorithms:<ul><li><code>RSA1_5</code> -
 RSA with PKCS#1 v1.5 padding.</li><li><code>RSA-OAEP</code> - RSA with Optimal Asymmetric Encryption
 Padding (OAEP) with SHA-1 and MGF-1.</li><li><code>RSA-OAEP-256</code> - RSA with OAEP with SHA-256
 and MGF-1.</li><li><code>A128KW</code> - AES Key Wrapping with 128-bit key derived from the client
 secret.</li><li><code>A192KW</code> - AES Key Wrapping with 192-bit key derived from the client
 secret.</li><li><code>A256KW</code> - AES Key Wrapping with 256-bit key derived from the client
 secret.</li><li><code>dir</code> - Direct encryption with AES using the hashed client secret.</li></
ul>",
          "propertyOrder" : 450,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "supportedRcsRequestEncryptionMethods" : {
          "title" : "Remote Consent Service Request Encryption Methods Supported",
          "description" : "Encryption methods supported to encrypt Remote Consent Service
 requests.<br><br>OpenAM supports the following encryption methods:<ul><li><code>A128GCM</code>,
 <code>A192GCM</code>, and <code>A256GCM</code> - AES in Galois Counter Mode (GCM) authenticated
 encryption mode.</li><li><code>A128CBC-HS256</code>, <code>A192CBC-HS384</code>, and <code>A256CBC-
HS512</code> - AES encryption in CBC mode, with HMAC-SHA-2 for integrity.</li></ul>",
          "propertyOrder" : 451,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "supportedRcsRequestSigningAlgorithms" : {
          "title" : "Remote Consent Service Request Signing Algorithms Supported",
          "description" : "Algorithms supported to sign consent_request JWTs for Remote Consent
 Services.<br><br>OpenAM supports signing algorithms listed in JSON Web Algorithms (JWA): <a href=
\"https://tools.ietf.org/html/rfc7518#section-3.1\">\"alg\" (Algorithm) Header Parameter Values
 for JWS</a>:<ul><li><code>HS256</code> - HMAC with SHA-256.</li><li><code>HS384</code> - HMAC with
 SHA-384.</li><li><code>HS512</code> - HMAC with SHA-512.</li><li><code>ES256</code> - ECDSA with
 SHA-256 and NIST standard P-256 elliptic curve.</li><li><code>ES384</code> - ECDSA with SHA-384 and
```

```
 NIST standard P-384 elliptic curve.</li><li><code>ES512</code> - ECDSA with SHA-512 and NIST standard
 P-521 elliptic curve.</li><li><code>RS256</code> - RSASSA-PKCS-v1_5 using SHA-256.</li></ul>",
          "propertyOrder" : 449,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "supportedRcsResponseSigningAlgorithms" : {
          "title" : "Remote Consent Service Response Signing Algorithms Supported",
          "description" : "Algorithms supported to verify signed consent_response JWT from Remote
 Consent Services.<br><br>OpenAM supports signing algorithms listed in JSON Web Algorithms (JWA): <a
 href=\"https://tools.ietf.org/html/rfc7518#section-3.1\">\"alg\" (Algorithm) Header Parameter Values
 for JWS</a>:<ul><li><code>HS256</code> - HMAC with SHA-256.</li><li><code>HS384</code> - HMAC with
 SHA-384.</li><li><code>HS512</code> - HMAC with SHA-512.</li><li><code>ES256</code> - ECDSA with
 SHA-256 and NIST standard P-256 elliptic curve.</li><li><code>ES384</code> - ECDSA with SHA-384 and
 NIST standard P-384 elliptic curve.</li><li><code>ES512</code> - ECDSA with SHA-512 and NIST standard
 P-521 elliptic curve.</li><li><code>RS256</code> - RSASSA-PKCS-v1_5 using SHA-256.</li></ul>",
          "propertyOrder" : 452,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "supportedRcsResponseEncryptionMethods" : {
          "title" : "Remote Consent Service Response Encryption Methods Supported",
          "description" : "Encryption methods supported to decrypt Remote Consent Service
 responses.<br><br>OpenAM supports the following encryption methods:<ul><li><code>A128GCM</code>,
 <code>A192GCM</code>, and <code>A256GCM</code> - AES in Galois Counter Mode (GCM) authenticated
 encryption mode.</li><li><code>A128CBC-HS256</code>, <code>A192CBC-HS384</code>, and <code>A256CBC-
HS512</code> - AES encryption in CBC mode, with HMAC-SHA-2 for integrity.</li></ul>",
          "propertyOrder" : 454,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "supportedRcsResponseEncryptionAlgorithms" : {
          "title" : "Remote Consent Service Response Encryption Algorithms Supported",
          "description" : "Encryption algorithms supported to decrypt Remote Consent Service
 responses.<br><br>OpenAM supports the following encryption algorithms:<ul><li><code>RSA1_5</code> -
 RSA with PKCS#1 v1.5 padding.</li><li><code>RSA-OAEP</code> - RSA with Optimal Asymmetric Encryption
 Padding (OAEP) with SHA-1 and MGF-1.</li><li><code>RSA-OAEP-256</code> - RSA with OAEP with SHA-256
 and MGF-1.</li><li><code>A128KW</code> - AES Key Wrapping with 128-bit key derived from the client
 secret.</li><li><code>A192KW</code> - AES Key Wrapping with 192-bit key derived from the client
 secret.</li><li><code>A256KW</code> - AES Key Wrapping with 256-bit key derived from the client
 secret.</li><li><code>dir</code> - Direct encryption with AES using the hashed client secret.</li></
ul>",
          "propertyOrder" : 453,
          "required" : true,
          "items" : {
            "type" : "string"
          },
```

```
          "type" : "array",
          "exampleValue" : ""
        },
        "remoteConsentServiceId" : {
          "title" : "Remote Consent Service ID",
          "description" : "The ID of an existing remote consent service agent.",
          "propertyOrder" : 448,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "enableRemoteConsent" : {
          "title" : "Enable Remote Consent",
          "description" : "",
          "propertyOrder" : 447,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "savedConsentAttribute" : {
          "title" : "Saved Consent Attribute Name",
          "description" : "Name of a multi-valued attribute on resource owner profiles where OpenAM
can save authorization consent decisions.<p><p>When the resource owner chooses to save the decision
to authorize access for a client application, then OpenAM updates the resource owner's profile to
avoid having to prompt the resource owner to grant authorization when the client issues subsequent
authorization requests.",
          "propertyOrder" : 110,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "clientsCanSkipConsent" : {
          "title" : "Allow Clients to Skip Consent",
          "description" : "If enabled, clients may be configured so that the resource owner will not
be asked for consent during authorization flows.",
          "propertyOrder" : 420,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        }
      }
    },
    "cibaConfig" : {
      "type" : "object",
      "title" : "CIBA",
      "propertyOrder" : 7,
      "properties" : {
        "cibaAuthReqIdLifetime" : {
          "title" : "Back Channel Authentication ID Lifetime (seconds)",
          "description" : "The time back channel authentication request id is valid for, in seconds.",
          "propertyOrder" : 700,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "supportedCibaSigningAlgorithms" : {
          "title" : "Signing Algorithms Supported",
          "description" : "Algorithms supported to sign the CIBA request parameter.<p><p>OpenAM
supports signing algorithms listed in JSON Web Algorithms (JWA): <a href=\"https://
```

```
tools.ietf.org/html/rfc7518#section-3.1\">\"alg\" (Algorithm) Header Parameter Values for JWS</
a>:<ul><li><code>ES256</code> - ECDSA with SHA-256 and NIST standard P-256 elliptic curve.</
li><li><code>PS256</code> - RSASSA-PSS using SHA-256.</li></ul>",
          "propertyOrder" : 900,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "cibaMinimumPollingInterval" : {
          "title" : "Polling Wait Interval (seconds)",
          "description" : "The minimum amount of time in seconds that the Client should wait between
 polling requests to the token endpoint",
          "propertyOrder" : 800,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        }
      }
    },
    "deviceCodeConfig" : {
      "type" : "object",
      "title" : "Device Flow",
      "propertyOrder" : 5,
      "properties" : {
        "verificationUrl" : {
          "title" : "Verification URL",
          "description" : "The URL that the user will be instructed to visit to complete their OAuth
 2.0 login and consent when using the device code flow.",
          "propertyOrder" : 370,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "deviceCodeLifetime" : {
          "title" : "Device Code Lifetime (seconds)",
          "description" : "The lifetime of the device code, in seconds.",
          "propertyOrder" : 390,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "devicePollInterval" : {
          "title" : "Device Polling Interval",
          "description" : "The polling frequency for devices waiting for tokens when using the device
 code flow.",
          "propertyOrder" : 400,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "completionUrl" : {
          "title" : "Device Completion URL",
          "description" : "The URL that the user will be sent to on completion of their OAuth 2.0
 login and consent when using the device code flow.",
          "propertyOrder" : 380,
          "required" : false,
```

```
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "coreOAuth2Config" : {
      "type" : "object",
      "title" : "Core",
      "propertyOrder" : 0,
      "properties" : {
        "issueRefreshToken" : {
          "title" : "Issue Refresh Tokens",
          "description" : "Whether to issue a refresh token when returning an access token.",
          "propertyOrder" : 40,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "statelessTokensEnabled" : {
          "title" : "Use Client-Based Access & Refresh Tokens",
          "description" : "When enabled, OpenAM issues access and refresh tokens that can be inspected
by resource servers.",
          "propertyOrder" : 3,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "issueRefreshTokenOnRefreshedToken" : {
          "title" : "Issue Refresh Tokens on Refreshing Access Tokens",
          "description" : "Whether to issue a refresh token when refreshing an access token.",
          "propertyOrder" : 50,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "usePolicyEngineForScope" : {
          "title" : "Use Policy Engine for Scope decisions",
          "description" : "With this setting enabled, the policy engine is consulted for each scope
value that is requested.<br><br>If a policy returns an action of GRANT=true, the scope is consented
automatically, and the user is not consulted in a user-interaction flow. If a policy returns an
action of GRANT=false, the scope is not added to any resulting token, and the user will not see it
in a user-interaction flow. If no policy returns a value for the GRANT action, then if the grant type
is user-facing (i.e. authorization or device code flows), the user is asked for consent (or saved
consent is used), and if the grant type is not user-facing (password or client credentials), the
scope is not added to any resulting token.",
          "propertyOrder" : 55,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "accessTokenModificationScript" : {
          "title" : "OAuth2 Access Token Modification Script",
          "description" : "The script that is executed when issuing an access token. The script can
change the access token's internal data structure to include or exclude particular fields.",
          "propertyOrder" : 75,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
```

```
       "codeLifetime" : {
         "title" : "Authorization Code Lifetime (seconds)",
         "description" : "The time an authorization code is valid for, in seconds.",
         "propertyOrder" : 10,
         "required" : true,
         "type" : "integer",
         "exampleValue" : ""
       },
       "macaroonTokensEnabled" : {
         "title" : "Use Macaroon Access and Refresh Tokens",
         "description" : "When enabled, AM will issue access and refresh tokens as Macaroons with
 caveats.",
         "propertyOrder" : 6,
         "required" : true,
         "type" : "boolean",
         "exampleValue" : ""
       },
       "refreshTokenLifetime" : {
         "title" : "Refresh Token Lifetime (seconds)",
         "description" : "The time in seconds a refresh token is valid for. If this field is set to
 <code>-1</code>, the refresh token will never expire.",
         "propertyOrder" : 20,
         "required" : true,
         "type" : "integer",
         "exampleValue" : ""
       },
       "accessTokenLifetime" : {
         "title" : "Access Token Lifetime (seconds)",
         "description" : "The time an access token is valid for, in seconds. Note that if you set the
 value to <code>0</code>, the access token will not be valid. A maximum lifetime of 600 seconds is
 recommended.",
         "propertyOrder" : 30,
         "required" : true,
         "type" : "integer",
         "exampleValue" : ""
       }
     }
   },
   "advancedOIDCConfig" : {
     "type" : "object",
     "title" : "Advanced OpenID Connect",
     "propertyOrder" : 4,
     "properties" : {
       "supportedUserInfoEncryptionEnc" : {
         "title" : "UserInfo Encryption Methods Supported",
         "description" : "Encryption methods supported by the UserInfo endpoint.<br><br>OpenAM
 supports the following UserInfo endpoint encryption methods:<ul><li><code>A128GCM</code>,
 <code>A192GCM</code>, and <code>A256GCM</code> - AES in Galois Counter Mode (GCM) authenticated
 encryption mode.</li><li><code>A128CBC-HS256</code>, <code>A192CBC-HS384</code>, and <code>A256CBC-
HS512</code> - AES encryption in CBC mode, with HMAC-SHA-2 for integrity.</li></ul>",
         "propertyOrder" : 458,
         "required" : true,
         "items" : {
           "type" : "string"
         },
         "type" : "array",
         "exampleValue" : ""
       },
       "supportedRequestParameterSigningAlgorithms" : {
```

```
          "title" : "Request Parameter Signing Algorithms Supported",
          "description" : "Algorithms supported to verify signature of Request parameterOpenAM
 supports signing algorithms listed in JSON Web Algorithms (JWA): <a href=\"https://
tools.ietf.org/html/rfc7518#section-3.1\">\"alg\" (Algorithm) Header Parameter Values for JWS</
a>:<ul><li><code>HS256</code> - HMAC with SHA-256.</li><li><code>HS384</code> - HMAC with SHA-384.</
li><li><code>HS512</code> - HMAC with SHA-512.</li><li><code>ES256</code> - ECDSA with SHA-256 and
 NIST standard P-256 elliptic curve.</li><li><code>ES384</code> - ECDSA with SHA-384 and NIST standard
 P-384 elliptic curve.</li><li><code>ES512</code> - ECDSA with SHA-512 and NIST standard P-521
 elliptic curve.</li><li><code>RS256</code> - RSASSA-PKCS-v1_5 using SHA-256.</li></ul>",
          "propertyOrder" : 441,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "storeOpsTokens" : {
          "title" : "Store Ops Tokens",
          "description" : "Whether OpenAM will store the <i>ops</i> tokens corresponding to OpenID
 Connect sessions in the CTS store. Note that session management related endpoints will not work when
 this setting is disabled.",
          "propertyOrder" : 410,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "supportedUserInfoSigningAlgorithms" : {
          "title" : "UserInfo Signing Algorithms Supported",
          "description" : "Algorithms supported to verify signature of the UserInfo endpoint.
 OpenAM supports signing algorithms listed in JSON Web Algorithms (JWA): <a href=\"https://
tools.ietf.org/html/rfc7518#section-3.1\">\"alg\" (Algorithm) Header Parameter Values for JWS</
a>:<ul><li><code>HS256</code> - HMAC with SHA-256.</li><li><code>HS384</code> - HMAC with SHA-384.</
li><li><code>HS512</code> - HMAC with SHA-512.</li><li><code>ES256</code> - ECDSA with SHA-256 and
 NIST standard P-256 elliptic curve.</li><li><code>ES384</code> - ECDSA with SHA-384 and NIST standard
 P-384 elliptic curve.</li><li><code>ES512</code> - ECDSA with SHA-512 and NIST standard P-521
 elliptic curve.</li><li><code>RS256</code> - RSASSA-PKCS-v1_5 using SHA-256.</li></ul>",
          "propertyOrder" : 456,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "authorisedOpenIdConnectSSOClients" : {
          "title" : "Authorized OIDC SSO Clients",
          "description" : "Clients authorized to use OpenID Connect ID tokens as SSO
 Tokens.<br><br>Allows clients to act with the full authority of the user. Grant this permission only
 to trusted clients.",
          "propertyOrder" : 446,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "includeAllKtyAlgCombinationsInJwksUri" : {
```

```
          "title" : "Include all kty and alg combinations in jwks_uri",
          "description" : "By default only distinct kid entries are returned in the jwks_uri
 and the alg property is not included.Enabling this flag will result in duplicate kid entries,
 each one specifying a different kty and alg combination. <a href=\"https://tools.ietf.org/html/
rfc7517#section-4.5\">RFC7517 distinct key KIDs</a>",
          "propertyOrder" : 630,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "amrMappings" : {
          "title" : "OpenID Connect id_token amr Values to Auth Module Mappings",
          "description" : "Specify <code>amr</code> values to be returned in the OpenID Connect
 <code>id_token</code>. Once authentication has completed, the authentication modules that were used
 from the authentication service will be mapped to the <code>amr</code> values. If you do not require
 <code>amr</code> values, or are not providing OpenID Connect tokens, leave this field blank.",
          "propertyOrder" : 330,
          "required" : false,
          "patternProperties" : {
            ".*" : { }
          },
          "type" : "object",
          "exampleValue" : ""
        },
        "supportedUserInfoEncryptionAlgorithms" : {
          "title" : "UserInfo Encryption Algorithms Supported",
          "description" : "Encryption algorithms supported by the UserInfo endpoint.<br><br>OpenAM
 supports the following UserInfo endpoint encryption algorithms:<ul><li><code>RSA-OAEP</code> - RSA
 with Optimal Asymmetric Encryption Padding (OAEP) with SHA-1 and MGF-1.</li><li><code>RSA-OAEP-256</
code> - RSA with OAEP with SHA-256 and MGF-1.</li><li><code>A128KW</code> - AES Key Wrapping with
 128-bit key derived from the client secret.</li><li><code>RSA1_5</code> - RSA with PKCS#1 v1.5
 padding.</li><li><code>A256KW</code> - AES Key Wrapping with 256-bit key derived from the client
 secret.</li><li><code>dir</code> - Direct encryption with AES using the hashed client secret.</
li><li><code>A192KW</code> - AES Key Wrapping with 192-bit key derived from the client secret.</li></
ul>",
          "propertyOrder" : 457,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "loaMapping" : {
          "title" : "OpenID Connect acr_values to Auth Chain Mapping",
          "description" : "Maps OpenID Connect ACR values to authentication chains. For more details,
 see the <a href=\"http://openid.net/specs/openid-connect-core-1_0.html#AuthRequest\" target=\"_blank
\">acr_values parameter</a> in the OpenID Connect authentication request specification.",
          "propertyOrder" : 310,
          "required" : false,
          "patternProperties" : {
            ".*" : { }
          },
          "type" : "object",
          "exampleValue" : ""
        },
        "supportedTokenEndpointAuthenticationSigningAlgorithms" : {
          "title" : "Supported Token Endpoint JWS Signing Algorithms.",
```

```
          "description" : "Supported JWS Signing Algorithms for 'private_key_jwt' JWT based
 authentication method.",
          "propertyOrder" : 444,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "defaultACR" : {
          "title" : "Default ACR values",
          "description" : "Default requested Authentication Context Class Reference
 values.<br><br>List of strings that specifies the default acr values that the OP is being requested
 to use for processing requests from this Client, with the values appearing in order of preference.
 The Authentication Context Class satisfied by the authentication performed is returned as the
 acr Claim Value in the issued ID Token. The acr Claim is requested as a Voluntary Claim by this
 parameter. The acr_values_supported discovery element contains a list of the acr values supported by
 this server. Values specified in the acr_values request parameter or an individual acr Claim request
 override these default values.",
          "propertyOrder" : 320,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "idTokenInfoClientAuthenticationEnabled" : {
          "title" : "Idtokeninfo Endpoint Requires Client Authentication",
          "description" : "When enabled, the <code>/oauth2/idtokeninfo</code> endpoint requires
 client authentication if the signing algorithm is set to <code>HS256</code>, <code>HS384</code>, or
 <code>HS512</code>.",
          "propertyOrder" : 225,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "supportedTokenIntrospectionResponseEncryptionEnc" : {
          "title" : "Token Introspection Response Encryption Methods Supported",
          "description" : "Encryption methods supported by the Token Introspection endpoint JWT
 response.<br><br>OpenAM supports the following encryption methods:<ul><li><code>A128GCM</code>,
 <code>A192GCM</code>, and <code>A256GCM</code> - AES in Galois Counter Mode (GCM) authenticated
 encryption mode.</li><li><code>A128CBC-HS256</code>, <code>A192CBC-HS384</code>, and <code>A256CBC-
HS512</code> - AES encryption in CBC mode, with HMAC-SHA-2 for integrity.</li></ul>",
          "propertyOrder" : 461,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "supportedRequestParameterEncryptionAlgorithms" : {
          "title" : "Request Parameter Encryption Algorithms Supported",
          "description" : "Encryption algorithms supported to decrypt Request parameter.<br><br>OpenAM
 supports the following ID token encryption algorithms:<ul><li><code>RSA-OAEP</code> - RSA with
 Optimal Asymmetric Encryption Padding (OAEP) with SHA-1 and MGF-1.</li><li><code>RSA-OAEP-256</
code> - RSA with OAEP with SHA-256 and MGF-1.</li><li><code>A128KW</code> - AES Key Wrapping with
```

```
 128-bit key derived from the client secret.</li><li><code>RSA1_5</code> - RSA with PKCS#1 v1.5
 padding.</li><li><code>A256KW</code> - AES Key Wrapping with 256-bit key derived from the client
 secret.</li><li><code>dir</code> - Direct encryption with AES using the hashed client secret.</
li><li><code>A192KW</code> - AES Key Wrapping with 192-bit key derived from the client secret.</li></
ul>",
          "propertyOrder" : 442,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "claimsParameterSupported" : {
          "title" : "Enable \"claims_parameter_supported\"",
          "description" : "If enabled, clients will be able to request individual claims using the
 <code>claims</code> request parameter, as per <a href=\"http://openid.net/specs/openid-connect-
core-1_0.html#ClaimsParameter\" target=\"_blank\">section 5.5 of the OpenID Connect specification</
a>.",
          "propertyOrder" : 250,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "supportedRequestParameterEncryptionEnc" : {
          "title" : "Request Parameter Encryption Methods Supported",
          "description" : "Encryption methods supported to decrypt Request parameter.<br><br>OpenAM
 supports the following Request parameter encryption algorithms:<ul><li><code>A128GCM</code>,
 <code>A192GCM</code>, and <code>A256GCM</code> - AES in Galois Counter Mode (GCM) authenticated
 encryption mode.</li><li><code>A128CBC-HS256</code>, <code>A192CBC-HS384</code>, and <code>A256CBC-
HS512</code> - AES encryption in CBC mode, with HMAC-SHA-2 for integrity.</li></ul>",
          "propertyOrder" : 443,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "supportedTokenIntrospectionResponseSigningAlgorithms" : {
          "title" : "Token Introspection Response Signing Algorithms Supported",
          "description" : "Algorithms that are supported for signing the Token Introspection endpoint
 JWT response.<br><br>OpenAM supports signing algorithms listed in JSON Web Algorithms (JWA): <a
 href=\"https://tools.ietf.org/html/rfc7518#section-3.1\">\"alg\" (Algorithm) Header Parameter Values
 for JWS</a>:<ul><li><code>HS256</code> - HMAC with SHA-256.</li><li><code>HS384</code> - HMAC with
 SHA-384.</li><li><code>HS512</code> - HMAC with SHA-512.</li><li><code>ES256</code> - ECDSA with
 SHA-256 and NIST standard P-256 elliptic curve.</li><li><code>ES384</code> - ECDSA with SHA-384
 and NIST standard P-384 elliptic curve.</li><li><code>ES512</code> - ECDSA with SHA-512 and NIST
 standard P-521 elliptic curve.</li><li><code>RS256</code> - RSASSA-PKCS-v1_5 using SHA-256.</
li><li><code>RS384</code> - RSASSA-PKCS-v1_5 using SHA-384.</li><li><code>RS512</code> - RSASSA-PKCS-
v1_5 using SHA-512.</li><li><code>EdDSA</code> - EdDSA with SHA-512.</li></ul>",
          "propertyOrder" : 459,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
```

```
        "alwaysAddClaimsToToken" : {
          "title" : "Always Return Claims in ID Tokens",
          "description" : "If enabled, include scope-derived claims in the <code>id_token</code>,
 even if an access token is also returned that could provide access to get the claims from the
 <code>userinfo</code> endpoint.<br><br>If not enabled, if an access token is requested the client
 must use it to access the <code>userinfo</code> endpoint for scope-derived claims, as they will not
 be included in the ID token.",
          "propertyOrder" : 360,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "jkwsURI" : {
          "title" : "Remote JSON Web Key URL",
          "description" : "The Remote URL where the providers JSON Web Key can be retrieved.<p><p>If
 this setting is not configured, then OpenAM provides a local URL to access the public key of the
 private key used to sign ID tokens.",
          "propertyOrder" : 140,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "supportedTokenIntrospectionResponseEncryptionAlgorithms" : {
          "title" : "Token Introspection Response Encryption Algorithms Supported",
          "description" : "Encryption algorithms supported by the Token Introspection
 endpoint JWT response.<br><br>OpenAM supports the following UserInfo endpoint encryption
 algorithms:<ul><li><code>RSA-OAEP</code> - RSA with Optimal Asymmetric Encryption Padding (OAEP)
 with SHA-1 and MGF-1.</li><li><code>RSA-OAEP-256</code> - RSA with OAEP with SHA-256 and MGF-1.</
li><li><code>A128KW</code> - AES Key Wrapping with 128-bit key derived from the client secret.</
li><li><code>RSA1_5</code> - RSA with PKCS#1 v1.5 padding.</li><li><code>A256KW</code> - AES
 Key Wrapping with 256-bit key derived from the client secret.</li><li><code>dir</code> - Direct
 encryption with AES using the hashed client secret.</li><li><code>A192KW</code> - AES Key Wrapping
 with 192-bit key derived from the client secret.</li></ul>",
          "propertyOrder" : 460,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        }
      }
    },
    "clientDynamicRegistrationConfig" : {
      "type" : "object",
      "title" : "Client Dynamic Registration",
      "propertyOrder" : 2,
      "properties" : {
        "dynamicClientRegistrationScope" : {
          "title" : "Scope to give access to dynamic client registration",
          "description" : "Mandatory scope required when registering a new OAuth2 client.",
          "propertyOrder" : 455,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "allowDynamicRegistration" : {
          "title" : "Allow Open Dynamic Client Registration",
```

```
          "description" : "Allow clients to register without an access token. If enabled, you
 should consider adding some form of rate limiting. For more information, see  <a href=\"https://
openid.net/specs/openid-connect-registration-1_0.html#ClientRegistration\" target=\"_blank\">Client
 Registration</a> in the OpenID Connect specification.",
          "propertyOrder" : 280,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "generateRegistrationAccessTokens" : {
          "title" : "Generate Registration Access Tokens",
          "description" : "Whether to generate Registration Access Tokens for clients that register by
 using open dynamic client registration. Such tokens allow the client to access the <a href=\"https://
openid.net/specs/openid-connect-registration-1_0.html#ClientConfigurationEndpoint\" target=\"_blank
\">Client Configuration Endpoint</a> as per the OpenID Connect specification. This setting has no
 effect if Allow Open Dynamic Client Registration is disabled.",
          "propertyOrder" : 290,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "requiredSoftwareStatementAttestedAttributes" : {
          "title" : "Required Software Statement Attested Attributes",
          "description" : "The client attributes that are required to be present in the software
 statement JWT when registering an OAuth 2.0 client dynamically. Only applies if Require Software
 Statements for Dynamic Client Registration is enabled.<br><br>Leave blank to allow any attributes to
 be present.",
          "propertyOrder" : 272,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "dynamicClientRegistrationSoftwareStatementRequired" : {
          "title" : "Require Software Statement for Dynamic Client Registration",
          "description" : "When enabled, a software statement JWT containing at least the <code>iss</
code> (issuer) claim must be provided when registering an OAuth 2.0 client dynamically.",
          "propertyOrder" : 271,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        }
      }
    },
    "coreOIDCConfig" : {
      "type" : "object",
      "title" : "OpenID Connect",
      "propertyOrder" : 3,
      "properties" : {
        "supportedClaims" : {
          "title" : "Supported Claims",
          "description" : "Set of claims supported by the OpenID Connect <code>/oauth2/userinfo</
code> endpoint, with translations.<br><br>Claims may be entered as simple strings or pipe separated
 strings representing the internal claim name, locale, and localized description.<p><p>For example:
 <code>name|en|Your full name.</code>.<p>Locale strings are in the format: <code>language +
 \"_\" + country + \"_\" + variant</code>, for example <code>en</code>, <code>en_GB</code>, or
 <code>en_US_WIN</code>. If the locale and pipe is omitted, the description is displayed to all users
```

```
 that have undefined locales.<p><p>If the description is also omitted, nothing is displayed on the
 consent page for the claim. For example specifying <code>family_name|</code> would allow the claim
 <code>family_name</code> to be used by the client, but would not display it to the user on the
 consent page when requested.",
          "propertyOrder" : 190,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "oidcDiscoveryEndpointEnabled" : {
          "title" : "OIDC Provider Discovery",
          "description" : "Turns on and off OIDC Discovery endpoint.",
          "propertyOrder" : 1000,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "oidcClaimsScript" : {
          "title" : "OIDC Claims Script",
          "description" : "The script that is run when issuing an ID token or making a request to the
 <i>userinfo</i> endpoint during OpenID requests.<p><p>The script gathers the scopes and populates
 claims, and has access to the access token, the user's identity and, if available, the user's
 session.",
          "propertyOrder" : 80,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "supportedIDTokenEncryptionMethods" : {
          "title" : "ID Token Encryption Methods supported",
          "description" : "Encryption methods supported to encrypt OpenID Connect ID tokens
 in order to hide its contents.<br><br>OpenAM supports the following ID token encryption
 algorithms:<ul><li><code>A128GCM</code>, <code>A192GCM</code>, and <code>A256GCM</code> - AES
 in Galois Counter Mode (GCM) authenticated encryption mode.</li><li><code>A128CBC-HS256</code>,
 <code>A192CBC-HS384</code>, and <code>A256CBC-HS512</code> - AES encryption in CBC mode, with HMAC-
SHA-2 for integrity.</li></ul>",
          "propertyOrder" : 180,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "supportedIDTokenEncryptionAlgorithms" : {
          "title" : "ID Token Encryption Algorithms supported",
          "description" : "Encryption algorithms supported to encrypt OpenID Connect ID tokens
 in order to hide its contents.<br><br>OpenAM supports the following ID token encryption
 algorithms:<ul><li><code>RSA-OAEP</code> - RSA with Optimal Asymmetric Encryption Padding (OAEP)
 with SHA-1 and MGF-1.</li><li><code>RSA-OAEP-256</code> - RSA with OAEP with SHA-256 and MGF-1.</
li><li><code>A128KW</code> - AES Key Wrapping with 128-bit key derived from the client secret.</
li><li><code>RSA1_5</code> - RSA with PKCS#1 v1.5 padding.</li><li><code>A256KW</code> - AES
 Key Wrapping with 256-bit key derived from the client secret.</li><li><code>dir</code> - Direct
 encryption with AES using the hashed client secret.</li><li><code>A192KW</code> - AES Key Wrapping
 with 192-bit key derived from the client secret.</li></ul>",
          "propertyOrder" : 170,
```

```
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "supportedIDTokenSigningAlgorithms" : {
          "title" : "ID Token Signing Algorithms supported",
          "description" : "Algorithms supported to sign OpenID Connect <code>id_tokens</
code>.<p><p>OpenAM supports signing algorithms listed in JSON Web Algorithms (JWA): <a href=\"https://
tools.ietf.org/html/rfc7518#section-3.1\">\"alg\" (Algorithm) Header Parameter Values for JWS</
a>:<ul><li><code>HS256</code> - HMAC with SHA-256.</li><li><code>HS384</code> - HMAC with SHA-384.</
li><li><code>HS512</code> - HMAC with SHA-512.</li><li><code>ES256</code> - ECDSA with SHA-256 and
 NIST standard P-256 elliptic curve.</li><li><code>ES384</code> - ECDSA with SHA-384 and NIST standard
 P-384 elliptic curve.</li><li><code>ES512</code> - ECDSA with SHA-512 and NIST standard P-521
 elliptic curve.</li><li><code>RS256</code> - RSASSA-PKCS-v1_5 using SHA-256.</li><li><code>RS384</
code> - RSASSA-PKCS-v1_5 using SHA-384.</li><li><code>RS512</code> - RSASSA-PKCS-v1_5 using SHA-512.</
li><li><code>PS256</code> - RSASSA-PSS using SHA-256.</li><li><code>PS384</code> - RSASSA-PSS using
 SHA-384.</li><li><code>PS512</code> - RSASSA-PSS using SHA-512.</li></ul>",
          "propertyOrder" : 160,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "jwtTokenLifetime" : {
          "title" : "OpenID Connect JWT Token Lifetime (seconds)",
          "description" : "The amount of time the JWT will be valid for, in seconds.",
          "propertyOrder" : 210,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        }
      }
    }
  }
}
```


delete

Usage:

```
am> delete OAuth2Provider --realm Realm
```

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action OAuth2Provider --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action OAuth2Provider --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action OAuth2Provider --realm Realm --actionName nextdescendents
```

read

Usage:

```
am> read OAuth2Provider --realm Realm
```

update

Usage:

```
am> update OAuth2Provider --realm Realm --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "advancedOAuth2Config" : {
      "type" : "object",
      "title" : "Advanced",
      "propertyOrder" : 1,
      "properties" : {
        "tlsCertificateRevocationCheckingEnabled" : {
          "title" : "Check TLS Certificate Revocation Status",
          "description" : "Whether to check if TLS client certificates have been revoked.<br><br>If
 enabled then AM will check if TLS client certificates used for client authentication have been
 revoked using either OCSP (preferred) or CRL. AM implements \"soft fail\" semantics: if the
 revocation status cannot be established due to a temporary error (e.g., network error) then the
 certificate is assumed to still be valid.",
          "propertyOrder" : 615,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
```

```
        },
        "tlsOcspResponderUri" : {
          "title" : "OCSP Responder URI",
          "description" : "URI of the OCSP responder service to use for checking certificate
 revocation status.<br><br>If specified this value overrides any OCSP or CRL mechanisms specified in
 individual certificates.",
          "propertyOrder" : 616,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "tlsClientCertificateTrustedHeader" : {
          "title" : "Trusted TLS Client Certificate Header",
          "description" : "HTTP Header to receive TLS client certificates when TLS is terminated at a
 proxy.<br><br>Leave blank if not terminating TLS at a proxy. Ensure that the proxy is configured to
 strip this headerfrom incoming requests. Best practice is to use a random string.",
          "propertyOrder" : 600,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "tlsOcspResponderCert" : {
          "title" : "OCSP Responder Certificate",
          "description" : "PEM-encoded certificate to use to verify OCSP responses.<br><br>If
 specified this certificate will be used to verify the signature on all OCSP responses. Otherwise the
 appropriate certificate will be determined from the trusted CA certificates.",
          "propertyOrder" : 617,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "codeVerifierEnforced" : {
          "title" : "Code Verifier Parameter Required",
          "description" : "If enabled, requests using the authorization code grant require a
 <code>code_challenge</code> attribute.<br><br>For more information, read the <a href=\"https://
tools.ietf.org/html/rfc7636\">specification for this feature</a>.",
          "propertyOrder" : 270,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "tokenEncryptionEnabled" : {
          "title" : "Encrypt Client-Based Tokens",
          "description" : "Whether client-based access and refresh tokens should be
 encrypted.<br><br>Enabling token encryption will disable token signing as encryption is performed
 using direct symmetric encryption.",
          "propertyOrder" : 242,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "passwordGrantAuthService" : {
          "title" : "Password Grant Authentication Service",
          "description" : "The authentication service (chain or tree) that will be used to
 authenticate the username and password for the resource owner password credentials grant type.",
          "propertyOrder" : 430,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
```

```
        },
        "tlsClientCertificateHeaderFormat" : {
          "title" : "TLS Client Certificate Header Format",
          "description" : "Format of the HTTP header used to communicate a client certificate
 from a reverse proxy.<br><br>The following formats are supported:<ul><li><code>URLENCODED_PEM</
code> - a URL-encoded PEM format certificate. This is the format used by Nginx.</
li><li><code>X_FORWARDED_CLIENT_CERT</code> - the <a target=\"_blank\" href=\"https://
www.envoyproxy.io/docs/envoy/latest/configuration/http/http_conn_man/headers#config-http-conn-man-
headers-x-forwarded-client-cert\">X-Forwarded-Client-Cert</a>format used by Envoy and Istio.</li></
ul>",
          "propertyOrder" : 605,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "displayNameAttribute" : {
          "title" : "User Display Name attribute",
          "description" : "The profile attribute that contains the name to be displayed for the user
 on the consent page.",
          "propertyOrder" : 120,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "createdTimestampAttribute" : {
          "title" : "Created Timestamp Attribute Name",
          "description" : "The identity Data Store attribute used to return created timestamp
 values.",
          "propertyOrder" : 350,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "supportedScopes" : {
          "title" : "Client Registration Scope Whitelist",
          "description" : "The set of scopes allowed when registering clients dynamically,
 with translations.<br><br><p>Scopes may be entered as simple strings or pipe-separated strings
 representing the internal scope name, locale, and localized description.</p><p>For example:
 <code>read|en|Permission to view email messages in your account</code></p><p>Locale strings are in
 the format: <code>language_country_variant</code>, for example <code>en</code>, <code>en_GB</code>,
 or <code>en_US_WIN</code>.</p><p>If the locale and pipe is omitted, the description is displayed
 to all users that have undefined locales.</p><p>If the description is also omitted, nothing is
 displayed on the consent page for the scope. For example specifying <code>read|</code> would allow
 the scope read to be used by the client, but would not display it to the user on the consent page
 when requested.</p>",
          "propertyOrder" : 130,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "allowedAudienceValues" : {
          "title" : "Additional Audience Values",
          "description" : "The additional audience values that will be permitted when verifying Client
 Authentication JWTs.<br><br>These audience values will be in addition to the AS base, issuer and
 endpoint URIs.",
          "propertyOrder" : 91,
```

```
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "modifiedTimestampAttribute" : {
          "title" : "Modified Timestamp Attribute Name",
          "description" : "The identity Data Store attribute used to return modified timestamp
 values.<p>This attribute is paired together with the <em>Created Timestamp Attribute Name</em>
 attribute (<code>createdTimestampAttribute</code>). You can leave both attributes unset (default) or
 set them both. If you set only one attribute and leave the other blank, the access token fails with
 a 500 error.<p>For example, when you configure AM as an OpenID Connect Provider in a Mobile Connect
 application and use DS as an identity data store, the client accesses the <code>userinfo</code>
 endpoint to obtain the <code>updated_at</code> claim value in the ID token. The <code>updated_at</
code> claim obtains its value from the <code>modifiedTimestampAttribute</code> attribute in the
 user profile. If the profile has never been modified the <code>updated_at</code> claim uses the
 <code>createdTimestampAttribute</code> attribute. ",
          "propertyOrder" : 340,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "responseTypeClasses" : {
          "title" : "Response Type Plugins",
          "description" : "List of plugins that handle the valid <code>response_type</code>
 values.<br><br>OAuth 2.0 clients pass response types as parameters to the OAuth 2.0 Authorization
 endpoint (<code>/oauth2/authorize</code>) to indicate which grant type is requested from the
 provider. For example, the client passes <code>code</code> when requesting an authorization code,
 and <code>token</code> when requesting an access token.<p><p>Values in this list take the form
 <code>response-type|plugin-class-name</code>.",
          "propertyOrder" : 90,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "customLoginUrlTemplate" : {
          "title" : "Custom Login URL Template",
          "description" : "Custom URL for handling login, to override the default OpenAM login
 page.<br><br>Supports Freemarker syntax, with the following variables:<table><tr><th>Variable</
th><th>Description</th></tr><tr><td><code>gotoUrl</code></td><td><p>The URL to redirect to after
 login.</p></td></tr><tr><td><code>acrValues</code></td><td><p>The Authentication Context Class
 Reference (acr) values for the authorization request.</p></td></tr><tr><td><code>realm</code></
td><td><p>The OpenAM realm the authorization request was made on.</p></td></tr><tr><td><code>module</
code></td><td><p>The name of the OpenAM authentication module requested to perform resource
 owner authentication.</p></td></tr><tr><td><code>service</code></td><td><p>The name of the
 OpenAM authentication chain requested to perform resource owner authentication.</p></td></
tr><tr><td><code>locale</code></td><td><p>A space-separated list of locales, ordered by
 preference.</p></td></tr></table>The following example template redirects users to a non-OpenAM
 front end to handle login, which will then redirect back to the <code>/oauth2/authorize</code>
 endpoint with any required parameters:<p> <code>http://mylogin.com/login?goto=${goto}&lt;#if
 acrValues??&gt;&amp;acr_values=${acrValues}&lt;&#x2F;#if&gt;&lt;#if realm??&gt;&amp;realm=
${realm}&lt;&#x2F;#if&gt;&lt;#if module??&gt;&amp;module=${module}&lt;&#x2F;#if&gt;&lt;#if
 service??&gt;&amp;service=${service}&lt;&#x2F;#if&gt;&lt;#if locale??&gt;&amp;locale=
```

```
${locale}&lt;&#x2F;#if&gt;</code><br><b>NOTE</b>: Default OpenAM login page is constructed using
 \"Base URL Source\" service.",
          "propertyOrder" : 60,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "moduleMessageEnabledInPasswordGrant" : {
          "title" : "Enable Auth Module Messages for Password Credentials Grant",
          "description" : "If enabled, authentication module failure messages are used to create
 Resource Owner Password Credentials Grant failure messages. If disabled, a standard authentication
 failed message is used.<br><br>The Password Grant Type requires the <code>grant_type=password</code>
 parameter.",
          "propertyOrder" : 440,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "hashSalt" : {
          "title" : "Subject Identifier Hash Salt",
          "description" : "If <i>pairwise</i> subject types are supported, it is <em>STRONGLY
 RECOMMENDED</em> to change this value. It is used in the salting of hashes for returning
 specific <code>sub</code> claims to individuals using the same <code>request_uri</code> or
 <code>sector_identifier_uri</code>.",
          "propertyOrder" : 260,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "supportedSubjectTypes" : {
          "title" : "Subject Types supported",
          "description" : "List of subject types supported. Valid values are:<ul><li><code>public</
code> - Each client receives the same subject (<code>sub</code>) value.</li><li><code>pairwise</code>
 - Each client receives a different subject (<code>sub</code>) value, to prevent correlation between
 clients.</li></ul>",
          "propertyOrder" : 150,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "scopeImplementationClass" : {
          "title" : "Scope Implementation Class",
          "description" : "The class that contains the required scope implementation, must implement
 the <code>org.forgerock.oauth2.core.ScopeValidator</code> interface.",
          "propertyOrder" : 70,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "tokenCompressionEnabled" : {
          "title" : "Client-Based Token Compression",
          "description" : "Whether client-based access and refresh tokens should be compressed.",
          "propertyOrder" : 223,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
```

```
        },
        "grantTypes" : {
          "title" : "Grant Types",
          "description" : "The set of Grant Types (OAuth2 Flows) that are permitted to be used by this
 client.<br><br>If no Grant Types (OAuth2 Flows) are configured nothing will be permitted.",
          "propertyOrder" : 560,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "macaroonTokenFormat" : {
          "title" : "Macaroon Token Format",
          "description" : "The format to use when serializing and parsing Macaroons. V1 is bulky and
 should only be used when compatibility with older Macaroon libraries is required.",
          "propertyOrder" : 620,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "authenticationAttributes" : {
          "title" : "User Profile Attribute(s) the Resource Owner is Authenticated On",
          "description" : "Names of profile attributes that resource owners use to log in. You can add
 others to the default, for example <code>mail</code>.",
          "propertyOrder" : 100,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "tokenSigningAlgorithm" : {
          "title" : "OAuth2 Token Signing Algorithm",
          "description" : "Algorithm used to sign client-based OAuth 2.0 tokens in order to detect
 tampering.<br><br>OpenAM supports signing algorithms listed in JSON Web Algorithms (JWA): <a href=
\"https://tools.ietf.org/html/rfc7518#section-3.1\">\"alg\" (Algorithm) Header Parameter Values for
 JWS</a>:<ul><li><code>HS256</code> - HMAC with SHA-256.</li><li><code>HS384</code> - HMAC with
 SHA-384.</li><li><code>HS512</code> - HMAC with SHA-512.</li><li><code>ES256</code> - ECDSA with
 SHA-256 and NIST standard P-256 elliptic curve.</li><li><code>ES384</code> - ECDSA with SHA-384 and
 NIST standard P-384 elliptic curve.</li><li><code>ES512</code> - ECDSA with SHA-512 and NIST standard
 P-521 elliptic curve.</li><li><code>RS256</code> - RSASSA-PKCS-v1_5 using SHA-256.</li></ul>",
          "propertyOrder" : 220,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "defaultScopes" : {
          "title" : "Default Client Scopes",
          "description" : "List of scopes a client will be granted if they request registration
 without specifying which scopes they want. Default scopes are NOT auto-granted to clients created
 through the OpenAM console.",
          "propertyOrder" : 200,
          "required" : false,
          "items" : {
            "type" : "string"
          },
```

```
          "type" : "array",
          "exampleValue" : ""
        },
        "tlsCertificateBoundAccessTokensEnabled" : {
          "title" : "Support TLS Certificate-Bound Access Tokens",
          "description" : "Whether to bind access tokens to the client certificate when using TLS
 client certificate authentication.",
          "propertyOrder" : 610,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        }
      }
    },
    "consent" : {
      "type" : "object",
      "title" : "Consent",
      "propertyOrder" : 6,
      "properties" : {
        "supportedRcsRequestEncryptionAlgorithms" : {
          "title" : "Remote Consent Service Request Encryption Algorithms Supported",
          "description" : "Encryption algorithms supported to encrypt Remote Consent Service
 requests.<br><br>OpenAM supports the following encryption algorithms:<ul><li><code>RSA1_5</code> -
 RSA with PKCS#1 v1.5 padding.</li><li><code>RSA-OAEP</code> - RSA with Optimal Asymmetric Encryption
 Padding (OAEP) with SHA-1 and MGF-1.</li><li><code>RSA-OAEP-256</code> - RSA with OAEP with SHA-256
 and MGF-1.</li><li><code>A128KW</code> - AES Key Wrapping with 128-bit key derived from the client
 secret.</li><li><code>A192KW</code> - AES Key Wrapping with 192-bit key derived from the client
 secret.</li><li><code>A256KW</code> - AES Key Wrapping with 256-bit key derived from the client
 secret.</li><li><code>dir</code> - Direct encryption with AES using the hashed client secret.</li></
ul>",
          "propertyOrder" : 450,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "supportedRcsRequestEncryptionMethods" : {
          "title" : "Remote Consent Service Request Encryption Methods Supported",
          "description" : "Encryption methods supported to encrypt Remote Consent Service
 requests.<br><br>OpenAM supports the following encryption methods:<ul><li><code>A128GCM</code>,
 <code>A192GCM</code>, and <code>A256GCM</code> - AES in Galois Counter Mode (GCM) authenticated
 encryption mode.</li><li><code>A128CBC-HS256</code>, <code>A192CBC-HS384</code>, and <code>A256CBC-
HS512</code> - AES encryption in CBC mode, with HMAC-SHA-2 for integrity.</li></ul>",
          "propertyOrder" : 451,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "supportedRcsRequestSigningAlgorithms" : {
          "title" : "Remote Consent Service Request Signing Algorithms Supported",
          "description" : "Algorithms supported to sign consent_request JWTs for Remote Consent
 Services.<br><br>OpenAM supports signing algorithms listed in JSON Web Algorithms (JWA): <a href=
\"https://tools.ietf.org/html/rfc7518#section-3.1\">\"alg\" (Algorithm) Header Parameter Values
 for JWS</a>:<ul><li><code>HS256</code> - HMAC with SHA-256.</li><li><code>HS384</code> - HMAC with
```

```
 SHA-384.</li><li><code>HS512</code> - HMAC with SHA-512.</li><li><code>ES256</code> - ECDSA with
 SHA-256 and NIST standard P-256 elliptic curve.</li><li><code>ES384</code> - ECDSA with SHA-384 and
 NIST standard P-384 elliptic curve.</li><li><code>ES512</code> - ECDSA with SHA-512 and NIST standard
 P-521 elliptic curve.</li><li><code>RS256</code> - RSASSA-PKCS-v1_5 using SHA-256.</li></ul>",
          "propertyOrder" : 449,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "supportedRcsResponseSigningAlgorithms" : {
          "title" : "Remote Consent Service Response Signing Algorithms Supported",
          "description" : "Algorithms supported to verify signed consent_response JWT from Remote
 Consent Services.<br><br>OpenAM supports signing algorithms listed in JSON Web Algorithms (JWA): <a
 href=\"https://tools.ietf.org/html/rfc7518#section-3.1\">\"alg\" (Algorithm) Header Parameter Values
 for JWS</a>:<ul><li><code>HS256</code> - HMAC with SHA-256.</li><li><code>HS384</code> - HMAC with
 SHA-384.</li><li><code>HS512</code> - HMAC with SHA-512.</li><li><code>ES256</code> - ECDSA with
 SHA-256 and NIST standard P-256 elliptic curve.</li><li><code>ES384</code> - ECDSA with SHA-384 and
 NIST standard P-384 elliptic curve.</li><li><code>ES512</code> - ECDSA with SHA-512 and NIST standard
 P-521 elliptic curve.</li><li><code>RS256</code> - RSASSA-PKCS-v1_5 using SHA-256.</li></ul>",
          "propertyOrder" : 452,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "supportedRcsResponseEncryptionMethods" : {
          "title" : "Remote Consent Service Response Encryption Methods Supported",
          "description" : "Encryption methods supported to decrypt Remote Consent Service
 responses.<br><br>OpenAM supports the following encryption methods:<ul><li><code>A128GCM</code>,
 <code>A192GCM</code>, and <code>A256GCM</code> - AES in Galois Counter Mode (GCM) authenticated
 encryption mode.</li><li><code>A128CBC-HS256</code>, <code>A192CBC-HS384</code>, and <code>A256CBC-
HS512</code> - AES encryption in CBC mode, with HMAC-SHA-2 for integrity.</li></ul>",
          "propertyOrder" : 454,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "supportedRcsResponseEncryptionAlgorithms" : {
          "title" : "Remote Consent Service Response Encryption Algorithms Supported",
          "description" : "Encryption algorithms supported to decrypt Remote Consent Service
 responses.<br><br>OpenAM supports the following encryption algorithms:<ul><li><code>RSA1_5</code> -
 RSA with PKCS#1 v1.5 padding.</li><li><code>RSA-OAEP</code> - RSA with Optimal Asymmetric Encryption
 Padding (OAEP) with SHA-1 and MGF-1.</li><li><code>RSA-OAEP-256</code> - RSA with OAEP with SHA-256
 and MGF-1.</li><li><code>A128KW</code> - AES Key Wrapping with 128-bit key derived from the client
 secret.</li><li><code>A192KW</code> - AES Key Wrapping with 192-bit key derived from the client
 secret.</li><li><code>A256KW</code> - AES Key Wrapping with 256-bit key derived from the client
 secret.</li><li><code>dir</code> - Direct encryption with AES using the hashed client secret.</li></
ul>",
          "propertyOrder" : 453,
          "required" : true,
          "items" : {
```

```
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "remoteConsentServiceId" : {
          "title" : "Remote Consent Service ID",
          "description" : "The ID of an existing remote consent service agent.",
          "propertyOrder" : 448,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "enableRemoteConsent" : {
          "title" : "Enable Remote Consent",
          "description" : "",
          "propertyOrder" : 447,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "savedConsentAttribute" : {
          "title" : "Saved Consent Attribute Name",
          "description" : "Name of a multi-valued attribute on resource owner profiles where OpenAM
can save authorization consent decisions.<p><p>When the resource owner chooses to save the decision
to authorize access for a client application, then OpenAM updates the resource owner's profile to
avoid having to prompt the resource owner to grant authorization when the client issues subsequent
authorization requests.",
          "propertyOrder" : 110,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "clientsCanSkipConsent" : {
          "title" : "Allow Clients to Skip Consent",
          "description" : "If enabled, clients may be configured so that the resource owner will not
be asked for consent during authorization flows.",
          "propertyOrder" : 420,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        }
      }
    },
    "cibaConfig" : {
      "type" : "object",
      "title" : "CIBA",
      "propertyOrder" : 7,
      "properties" : {
        "cibaAuthReqIdLifetime" : {
          "title" : "Back Channel Authentication ID Lifetime (seconds)",
          "description" : "The time back channel authentication request id is valid for, in seconds.",
          "propertyOrder" : 700,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "supportedCibaSigningAlgorithms" : {
          "title" : "Signing Algorithms Supported",
```

```
          "description" : "Algorithms supported to sign the CIBA request parameter.<p><p>OpenAM
 supports signing algorithms listed in JSON Web Algorithms (JWA): <a href=\"https://
tools.ietf.org/html/rfc7518#section-3.1\">\"alg\" (Algorithm) Header Parameter Values for JWS</
a>:<ul><li><code>ES256</code> - ECDSA with SHA-256 and NIST standard P-256 elliptic curve.</
li><li><code>PS256</code> - RSASSA-PSS using SHA-256.</li></ul>",
          "propertyOrder" : 900,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "cibaMinimumPollingInterval" : {
          "title" : "Polling Wait Interval (seconds)",
          "description" : "The minimum amount of time in seconds that the Client should wait between
 polling requests to the token endpoint",
          "propertyOrder" : 800,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        }
      }
    },
    "deviceCodeConfig" : {
      "type" : "object",
      "title" : "Device Flow",
      "propertyOrder" : 5,
      "properties" : {
        "verificationUrl" : {
          "title" : "Verification URL",
          "description" : "The URL that the user will be instructed to visit to complete their OAuth
 2.0 login and consent when using the device code flow.",
          "propertyOrder" : 370,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "deviceCodeLifetime" : {
          "title" : "Device Code Lifetime (seconds)",
          "description" : "The lifetime of the device code, in seconds.",
          "propertyOrder" : 390,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "devicePollInterval" : {
          "title" : "Device Polling Interval",
          "description" : "The polling frequency for devices waiting for tokens when using the device
 code flow.",
          "propertyOrder" : 400,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "completionUrl" : {
          "title" : "Device Completion URL",
          "description" : "The URL that the user will be sent to on completion of their OAuth 2.0
 login and consent when using the device code flow.",
```

```
          "propertyOrder" : 380,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "coreOAuth2Config" : {
      "type" : "object",
      "title" : "Core",
      "propertyOrder" : 0,
      "properties" : {
        "issueRefreshToken" : {
          "title" : "Issue Refresh Tokens",
          "description" : "Whether to issue a refresh token when returning an access token.",
          "propertyOrder" : 40,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "statelessTokensEnabled" : {
          "title" : "Use Client-Based Access & Refresh Tokens",
          "description" : "When enabled, OpenAM issues access and refresh tokens that can be inspected
by resource servers.",
          "propertyOrder" : 3,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "issueRefreshTokenOnRefreshedToken" : {
          "title" : "Issue Refresh Tokens on Refreshing Access Tokens",
          "description" : "Whether to issue a refresh token when refreshing an access token.",
          "propertyOrder" : 50,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "usePolicyEngineForScope" : {
          "title" : "Use Policy Engine for Scope decisions",
          "description" : "With this setting enabled, the policy engine is consulted for each scope
value that is requested.<br><br>If a policy returns an action of GRANT=true, the scope is consented
automatically, and the user is not consulted in a user-interaction flow. If a policy returns an
action of GRANT=false, the scope is not added to any resulting token, and the user will not see it
in a user-interaction flow. If no policy returns a value for the GRANT action, then if the grant type
is user-facing (i.e. authorization or device code flows), the user is asked for consent (or saved
consent is used), and if the grant type is not user-facing (password or client credentials), the
scope is not added to any resulting token.",
          "propertyOrder" : 55,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "accessTokenModificationScript" : {
          "title" : "OAuth2 Access Token Modification Script",
          "description" : "The script that is executed when issuing an access token. The script can
change the access token's internal data structure to include or exclude particular fields.",
          "propertyOrder" : 75,
          "required" : true,
          "type" : "string",
```

```
          "exampleValue" : ""
        },
        "codeLifetime" : {
          "title" : "Authorization Code Lifetime (seconds)",
          "description" : "The time an authorization code is valid for, in seconds.",
          "propertyOrder" : 10,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "macaroonTokensEnabled" : {
          "title" : "Use Macaroon Access and Refresh Tokens",
          "description" : "When enabled, AM will issue access and refresh tokens as Macaroons with
 caveats.",
          "propertyOrder" : 6,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "refreshTokenLifetime" : {
          "title" : "Refresh Token Lifetime (seconds)",
          "description" : "The time in seconds a refresh token is valid for. If this field is set to
 <code>-1</code>, the refresh token will never expire.",
          "propertyOrder" : 20,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "accessTokenLifetime" : {
          "title" : "Access Token Lifetime (seconds)",
          "description" : "The time an access token is valid for, in seconds. Note that if you set the
 value to <code>0</code>, the access token will not be valid. A maximum lifetime of 600 seconds is
 recommended.",
          "propertyOrder" : 30,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        }
      }
    },
    "advancedOIDCConfig" : {
      "type" : "object",
      "title" : "Advanced OpenID Connect",
      "propertyOrder" : 4,
      "properties" : {
        "supportedUserInfoEncryptionEnc" : {
          "title" : "UserInfo Encryption Methods Supported",
          "description" : "Encryption methods supported by the UserInfo endpoint.<br><br>OpenAM
 supports the following UserInfo endpoint encryption methods:<ul><li><code>A128GCM</code>,
 <code>A192GCM</code>, and <code>A256GCM</code> - AES in Galois Counter Mode (GCM) authenticated
 encryption mode.</li><li><code>A128CBC-HS256</code>, <code>A192CBC-HS384</code>, and <code>A256CBC-
HS512</code> - AES encryption in CBC mode, with HMAC-SHA-2 for integrity.</li></ul>",
          "propertyOrder" : 458,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
```

```
        },
        "supportedRequestParameterSigningAlgorithms" : {
          "title" : "Request Parameter Signing Algorithms Supported",
          "description" : "Algorithms supported to verify signature of Request parameterOpenAM
 supports signing algorithms listed in JSON Web Algorithms (JWA): <a href=\"https://
tools.ietf.org/html/rfc7518#section-3.1\">\"alg\" (Algorithm) Header Parameter Values for JWS</
a>:<ul><li><code>HS256</code> - HMAC with SHA-256.</li><li><code>HS384</code> - HMAC with SHA-384.</
li><li><code>HS512</code> - HMAC with SHA-512.</li><li><code>ES256</code> - ECDSA with SHA-256 and
 NIST standard P-256 elliptic curve.</li><li><code>ES384</code> - ECDSA with SHA-384 and NIST standard
 P-384 elliptic curve.</li><li><code>ES512</code> - ECDSA with SHA-512 and NIST standard P-521
 elliptic curve.</li><li><code>RS256</code> - RSASSA-PKCS-v1_5 using SHA-256.</li></ul>",
          "propertyOrder" : 441,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "storeOpsTokens" : {
          "title" : "Store Ops Tokens",
          "description" : "Whether OpenAM will store the <i>ops</i> tokens corresponding to OpenID
 Connect sessions in the CTS store. Note that session management related endpoints will not work when
 this setting is disabled.",
          "propertyOrder" : 410,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "supportedUserInfoSigningAlgorithms" : {
          "title" : "UserInfo Signing Algorithms Supported",
          "description" : "Algorithms supported to verify signature of the UserInfo endpoint.
 OpenAM supports signing algorithms listed in JSON Web Algorithms (JWA): <a href=\"https://
tools.ietf.org/html/rfc7518#section-3.1\">\"alg\" (Algorithm) Header Parameter Values for JWS</
a>:<ul><li><code>HS256</code> - HMAC with SHA-256.</li><li><code>HS384</code> - HMAC with SHA-384.</
li><li><code>HS512</code> - HMAC with SHA-512.</li><li><code>ES256</code> - ECDSA with SHA-256 and
 NIST standard P-256 elliptic curve.</li><li><code>ES384</code> - ECDSA with SHA-384 and NIST standard
 P-384 elliptic curve.</li><li><code>ES512</code> - ECDSA with SHA-512 and NIST standard P-521
 elliptic curve.</li><li><code>RS256</code> - RSASSA-PKCS-v1_5 using SHA-256.</li></ul>",
          "propertyOrder" : 456,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "authorisedOpenIdConnectSSOClients" : {
          "title" : "Authorized OIDC SSO Clients",
          "description" : "Clients authorized to use OpenID Connect ID tokens as SSO
 Tokens.<br><br>Allows clients to act with the full authority of the user. Grant this permission only
 to trusted clients.",
          "propertyOrder" : 446,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
```

```
        },
        "includeAllKtyAlgCombinationsInJwksUri" : {
          "title" : "Include all kty and alg combinations in jwks_uri",
          "description" : "By default only distinct kid entries are returned in the jwks_uri
 and the alg property is not included.Enabling this flag will result in duplicate kid entries,
 each one specifying a different kty and alg combination. <a href=\"https://tools.ietf.org/html/
rfc7517#section-4.5\">RFC7517 distinct key KIDs</a>",
          "propertyOrder" : 630,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "amrMappings" : {
          "title" : "OpenID Connect id_token amr Values to Auth Module Mappings",
          "description" : "Specify <code>amr</code> values to be returned in the OpenID Connect
 <code>id_token</code>. Once authentication has completed, the authentication modules that were used
 from the authentication service will be mapped to the <code>amr</code> values. If you do not require
 <code>amr</code> values, or are not providing OpenID Connect tokens, leave this field blank.",
          "propertyOrder" : 330,
          "required" : false,
          "patternProperties" : {
            ".*" : { }
          },
          "type" : "object",
          "exampleValue" : ""
        },
        "supportedUserInfoEncryptionAlgorithms" : {
          "title" : "UserInfo Encryption Algorithms Supported",
          "description" : "Encryption algorithms supported by the UserInfo endpoint.<br><br>OpenAM
 supports the following UserInfo endpoint encryption algorithms:<ul><li><code>RSA-OAEP</code> - RSA
 with Optimal Asymmetric Encryption Padding (OAEP) with SHA-1 and MGF-1.</li><li><code>RSA-OAEP-256</
code> - RSA with OAEP with SHA-256 and MGF-1.</li><li><code>A128KW</code> - AES Key Wrapping with
 128-bit key derived from the client secret.</li><li><code>RSA1_5</code> - RSA with PKCS#1 v1.5
 padding.</li><li><code>A256KW</code> - AES Key Wrapping with 256-bit key derived from the client
 secret.</li><li><code>dir</code> - Direct encryption with AES using the hashed client secret.</
li><li><code>A192KW</code> - AES Key Wrapping with 192-bit key derived from the client secret.</li></
ul>",
          "propertyOrder" : 457,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "loaMapping" : {
          "title" : "OpenID Connect acr_values to Auth Chain Mapping",
          "description" : "Maps OpenID Connect ACR values to authentication chains. For more details,
 see the <a href=\"http://openid.net/specs/openid-connect-core-1_0.html#AuthRequest\" target=\"_blank
\">acr_values parameter</a> in the OpenID Connect authentication request specification.",
          "propertyOrder" : 310,
          "required" : false,
          "patternProperties" : {
            ".*" : { }
          },
          "type" : "object",
          "exampleValue" : ""
        },
        "supportedTokenEndpointAuthenticationSigningAlgorithms" : {
```

```
          "title" : "Supported Token Endpoint JWS Signing Algorithms.",
          "description" : "Supported JWS Signing Algorithms for 'private_key_jwt' JWT based
 authentication method.",
          "propertyOrder" : 444,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "defaultACR" : {
          "title" : "Default ACR values",
          "description" : "Default requested Authentication Context Class Reference
 values.<br><br>List of strings that specifies the default acr values that the OP is being requested
 to use for processing requests from this Client, with the values appearing in order of preference.
 The Authentication Context Class satisfied by the authentication performed is returned as the
 acr Claim Value in the issued ID Token. The acr Claim is requested as a Voluntary Claim by this
 parameter. The acr_values_supported discovery element contains a list of the acr values supported by
 this server. Values specified in the acr_values request parameter or an individual acr Claim request
 override these default values.",
          "propertyOrder" : 320,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "idTokenInfoClientAuthenticationEnabled" : {
          "title" : "Idtokeninfo Endpoint Requires Client Authentication",
          "description" : "When enabled, the <code>/oauth2/idtokeninfo</code> endpoint requires
 client authentication if the signing algorithm is set to <code>HS256</code>, <code>HS384</code>, or
 <code>HS512</code>.",
          "propertyOrder" : 225,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "supportedTokenIntrospectionResponseEncryptionEnc" : {
          "title" : "Token Introspection Response Encryption Methods Supported",
          "description" : "Encryption methods supported by the Token Introspection endpoint JWT
 response.<br><br>OpenAM supports the following encryption methods:<ul><li><code>A128GCM</code>,
 <code>A192GCM</code>, and <code>A256GCM</code> - AES in Galois Counter Mode (GCM) authenticated
 encryption mode.</li><li><code>A128CBC-HS256</code>, <code>A192CBC-HS384</code>, and <code>A256CBC-
HS512</code> - AES encryption in CBC mode, with HMAC-SHA-2 for integrity.</li></ul>",
          "propertyOrder" : 461,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "supportedRequestParameterEncryptionAlgorithms" : {
          "title" : "Request Parameter Encryption Algorithms Supported",
          "description" : "Encryption algorithms supported to decrypt Request parameter.<br><br>OpenAM
 supports the following ID token encryption algorithms:<ul><li><code>RSA-OAEP</code> - RSA with
 Optimal Asymmetric Encryption Padding (OAEP) with SHA-1 and MGF-1.</li><li><code>RSA-OAEP-256</
```

```
code> - RSA with OAEP with SHA-256 and MGF-1.</li><li><code>A128KW</code> - AES Key Wrapping with
 128-bit key derived from the client secret.</li><li><code>RSA1_5</code> - RSA with PKCS#1 v1.5
 padding.</li><li><code>A256KW</code> - AES Key Wrapping with 256-bit key derived from the client
 secret.</li><li><code>dir</code> - Direct encryption with AES using the hashed client secret.</
li><li><code>A192KW</code> - AES Key Wrapping with 192-bit key derived from the client secret.</li></
ul>",
          "propertyOrder" : 442,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "claimsParameterSupported" : {
          "title" : "Enable \"claims_parameter_supported\"",
          "description" : "If enabled, clients will be able to request individual claims using the
 <code>claims</code> request parameter, as per <a href=\"http://openid.net/specs/openid-connect-
core-1_0.html#ClaimsParameter\" target=\"_blank\">section 5.5 of the OpenID Connect specification</
a>.",
          "propertyOrder" : 250,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "supportedRequestParameterEncryptionEnc" : {
          "title" : "Request Parameter Encryption Methods Supported",
          "description" : "Encryption methods supported to decrypt Request parameter.<br><br>OpenAM
 supports the following Request parameter encryption algorithms:<ul><li><code>A128GCM</code>,
 <code>A192GCM</code>, and <code>A256GCM</code> - AES in Galois Counter Mode (GCM) authenticated
 encryption mode.</li><li><code>A128CBC-HS256</code>, <code>A192CBC-HS384</code>, and <code>A256CBC-
HS512</code> - AES encryption in CBC mode, with HMAC-SHA-2 for integrity.</li></ul>",
          "propertyOrder" : 443,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "supportedTokenIntrospectionResponseSigningAlgorithms" : {
          "title" : "Token Introspection Response Signing Algorithms Supported",
          "description" : "Algorithms that are supported for signing the Token Introspection endpoint
 JWT response.<br><br>OpenAM supports signing algorithms listed in JSON Web Algorithms (JWA): <a
 href=\"https://tools.ietf.org/html/rfc7518#section-3.1\">\"alg\" (Algorithm) Header Parameter Values
 for JWS</a>:<ul><li><code>HS256</code> - HMAC with SHA-256.</li><li><code>HS384</code> - HMAC with
 SHA-384.</li><li><code>HS512</code> - HMAC with SHA-512.</li><li><code>ES256</code> - ECDSA with
 SHA-256 and NIST standard P-256 elliptic curve.</li><li><code>ES384</code> - ECDSA with SHA-384
 and NIST standard P-384 elliptic curve.</li><li><code>ES512</code> - ECDSA with SHA-512 and NIST
 standard P-521 elliptic curve.</li><li><code>RS256</code> - RSASSA-PKCS-v1_5 using SHA-256.</
li><li><code>RS384</code> - RSASSA-PKCS-v1_5 using SHA-384.</li><li><code>RS512</code> - RSASSA-PKCS-
v1_5 using SHA-512.</li><li><code>EdDSA</code> - EdDSA with SHA-512.</li></ul>",
          "propertyOrder" : 459,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
```

```
        },
        "alwaysAddClaimsToToken" : {
          "title" : "Always Return Claims in ID Tokens",
          "description" : "If enabled, include scope-derived claims in the <code>id_token</code>,
 even if an access token is also returned that could provide access to get the claims from the
 <code>userinfo</code> endpoint.<br><br>If not enabled, if an access token is requested the client
 must use it to access the <code>userinfo</code> endpoint for scope-derived claims, as they will not
 be included in the ID token.",
          "propertyOrder" : 360,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "jkwsURI" : {
          "title" : "Remote JSON Web Key URL",
          "description" : "The Remote URL where the providers JSON Web Key can be retrieved.<p><p>If
 this setting is not configured, then OpenAM provides a local URL to access the public key of the
 private key used to sign ID tokens.",
          "propertyOrder" : 140,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "supportedTokenIntrospectionResponseEncryptionAlgorithms" : {
          "title" : "Token Introspection Response Encryption Algorithms Supported",
          "description" : "Encryption algorithms supported by the Token Introspection
 endpoint JWT response.<br><br>OpenAM supports the following UserInfo endpoint encryption
 algorithms:<ul><li><code>RSA-OAEP</code> - RSA with Optimal Asymmetric Encryption Padding (OAEP)
 with SHA-1 and MGF-1.</li><li><code>RSA-OAEP-256</code> - RSA with OAEP with SHA-256 and MGF-1.</
li><li><code>A128KW</code> - AES Key Wrapping with 128-bit key derived from the client secret.</
li><li><code>RSA1_5</code> - RSA with PKCS#1 v1.5 padding.</li><li><code>A256KW</code> - AES
 Key Wrapping with 256-bit key derived from the client secret.</li><li><code>dir</code> - Direct
 encryption with AES using the hashed client secret.</li><li><code>A192KW</code> - AES Key Wrapping
 with 192-bit key derived from the client secret.</li></ul>",
          "propertyOrder" : 460,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        }
      }
    },
    "clientDynamicRegistrationConfig" : {
      "type" : "object",
      "title" : "Client Dynamic Registration",
      "propertyOrder" : 2,
      "properties" : {
        "dynamicClientRegistrationScope" : {
          "title" : "Scope to give access to dynamic client registration",
          "description" : "Mandatory scope required when registering a new OAuth2 client.",
          "propertyOrder" : 455,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "allowDynamicRegistration" : {
          "title" : "Allow Open Dynamic Client Registration",
```

```
          "description" : "Allow clients to register without an access token. If enabled, you
 should consider adding some form of rate limiting. For more information, see  <a href=\"https://
openid.net/specs/openid-connect-registration-1_0.html#ClientRegistration\" target=\"_blank\">Client
 Registration</a> in the OpenID Connect specification.",
          "propertyOrder" : 280,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "generateRegistrationAccessTokens" : {
          "title" : "Generate Registration Access Tokens",
          "description" : "Whether to generate Registration Access Tokens for clients that register by
 using open dynamic client registration. Such tokens allow the client to access the <a href=\"https://
openid.net/specs/openid-connect-registration-1_0.html#ClientConfigurationEndpoint\" target=\"_blank
\">Client Configuration Endpoint</a> as per the OpenID Connect specification. This setting has no
 effect if Allow Open Dynamic Client Registration is disabled.",
          "propertyOrder" : 290,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "requiredSoftwareStatementAttestedAttributes" : {
          "title" : "Required Software Statement Attested Attributes",
          "description" : "The client attributes that are required to be present in the software
 statement JWT when registering an OAuth 2.0 client dynamically. Only applies if Require Software
 Statements for Dynamic Client Registration is enabled.<br><br>Leave blank to allow any attributes to
 be present.",
          "propertyOrder" : 272,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "dynamicClientRegistrationSoftwareStatementRequired" : {
          "title" : "Require Software Statement for Dynamic Client Registration",
          "description" : "When enabled, a software statement JWT containing at least the <code>iss</
code> (issuer) claim must be provided when registering an OAuth 2.0 client dynamically.",
          "propertyOrder" : 271,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        }
      }
    },
    "coreOIDCConfig" : {
      "type" : "object",
      "title" : "OpenID Connect",
      "propertyOrder" : 3,
      "properties" : {
        "supportedClaims" : {
          "title" : "Supported Claims",
          "description" : "Set of claims supported by the OpenID Connect <code>/oauth2/userinfo</
code> endpoint, with translations.<br><br>Claims may be entered as simple strings or pipe separated
 strings representing the internal claim name, locale, and localized description.<p><p>For example:
 <code>name|en|Your full name.</code>.<p>Locale strings are in the format: <code>language +
 \"_\" + country + \"_\" + variant</code>, for example <code>en</code>, <code>en_GB</code>, or
 <code>en_US_WIN</code>. If the locale and pipe is omitted, the description is displayed to all users
```

```
 that have undefined locales.<p><p>If the description is also omitted, nothing is displayed on the
 consent page for the claim. For example specifying <code>family_name|</code> would allow the claim
 <code>family_name</code> to be used by the client, but would not display it to the user on the
 consent page when requested.",
          "propertyOrder" : 190,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "oidcDiscoveryEndpointEnabled" : {
          "title" : "OIDC Provider Discovery",
          "description" : "Turns on and off OIDC Discovery endpoint.",
          "propertyOrder" : 1000,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "oidcClaimsScript" : {
          "title" : "OIDC Claims Script",
          "description" : "The script that is run when issuing an ID token or making a request to the
 <i>userinfo</i> endpoint during OpenID requests.<p><p>The script gathers the scopes and populates
 claims, and has access to the access token, the user's identity and, if available, the user's
 session.",
          "propertyOrder" : 80,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "supportedIDTokenEncryptionMethods" : {
          "title" : "ID Token Encryption Methods supported",
          "description" : "Encryption methods supported to encrypt OpenID Connect ID tokens
 in order to hide its contents.<br><br>OpenAM supports the following ID token encryption
 algorithms:<ul><li><code>A128GCM</code>, <code>A192GCM</code>, and <code>A256GCM</code> - AES
 in Galois Counter Mode (GCM) authenticated encryption mode.</li><li><code>A128CBC-HS256</code>,
 <code>A192CBC-HS384</code>, and <code>A256CBC-HS512</code> - AES encryption in CBC mode, with HMAC-
SHA-2 for integrity.</li></ul>",
          "propertyOrder" : 180,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "supportedIDTokenEncryptionAlgorithms" : {
          "title" : "ID Token Encryption Algorithms supported",
          "description" : "Encryption algorithms supported to encrypt OpenID Connect ID tokens
 in order to hide its contents.<br><br>OpenAM supports the following ID token encryption
 algorithms:<ul><li><code>RSA-OAEP</code> - RSA with Optimal Asymmetric Encryption Padding (OAEP)
 with SHA-1 and MGF-1.</li><li><code>RSA-OAEP-256</code> - RSA with OAEP with SHA-256 and MGF-1.</
li><li><code>A128KW</code> - AES Key Wrapping with 128-bit key derived from the client secret.</
li><li><code>RSA1_5</code> - RSA with PKCS#1 v1.5 padding.</li><li><code>A256KW</code> - AES
 Key Wrapping with 256-bit key derived from the client secret.</li><li><code>dir</code> - Direct
 encryption with AES using the hashed client secret.</li><li><code>A192KW</code> - AES Key Wrapping
 with 192-bit key derived from the client secret.</li></ul>",
          "propertyOrder" : 170,
```

```
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "supportedIDTokenSigningAlgorithms" : {
          "title" : "ID Token Signing Algorithms supported",
          "description" : "Algorithms supported to sign OpenID Connect <code>id_tokens</
code>.<p><p>OpenAM supports signing algorithms listed in JSON Web Algorithms (JWA): <a href=\"https://
tools.ietf.org/html/rfc7518#section-3.1\">\"alg\" (Algorithm) Header Parameter Values for JWS</
a>:<ul><li><code>HS256</code> - HMAC with SHA-256.</li><li><code>HS384</code> - HMAC with SHA-384.</
li><li><code>HS512</code> - HMAC with SHA-512.</li><li><code>ES256</code> - ECDSA with SHA-256 and
 NIST standard P-256 elliptic curve.</li><li><code>ES384</code> - ECDSA with SHA-384 and NIST standard
 P-384 elliptic curve.</li><li><code>ES512</code> - ECDSA with SHA-512 and NIST standard P-521
 elliptic curve.</li><li><code>RS256</code> - RSASSA-PKCS-v1_5 using SHA-256.</li><li><code>RS384</
code> - RSASSA-PKCS-v1_5 using SHA-384.</li><li><code>RS512</code> - RSASSA-PKCS-v1_5 using SHA-512.</
li><li><code>PS256</code> - RSASSA-PSS using SHA-256.</li><li><code>PS384</code> - RSASSA-PSS using
 SHA-384.</li><li><code>PS512</code> - RSASSA-PSS using SHA-512.</li></ul>",
          "propertyOrder" : 160,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "jwtTokenLifetime" : {
          "title" : "OpenID Connect JWT Token Lifetime (seconds)",
          "description" : "The amount of time the JWT will be valid for, in seconds.",
          "propertyOrder" : 210,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        }
      }
    }
  }
}
```


Global Operations

Resource path: `/global-config/services/oauth-oidc`

Resource version: `1.0`

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action OAuth2Provider --global --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action OAuth2Provider --global --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action OAuth2Provider --global --actionName nextdescendents
```

read

Usage:

```
am> read OAuth2Provider --global
```

update

Usage:

```
am> update OAuth2Provider --global --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "storageScheme" : {
      "title" : "CTS Storage Scheme",
      "description" : "Storage scheme to be used when storing OAuth2 tokens to CTS.<br><br>In order
 to support rolling upgrades, this should be set to the latest storage scheme supported by all OpenAM
 instances within your cluster. Select the latest storage scheme once all OpenAM instances in the
 cluster have been upgraded.<br/><br/><b>One-to-One Storage Scheme</b><br/>Under this storage scheme,
 each OAuth2 token maps to an individual CTS entry.<br/><i>This storage scheme is inefficient - use
 the Grant-Set Storage Scheme once all servers have been upgraded to a version which supports it.</
i><br/><br/><b>Grant-Set Storage Scheme</b><br/>Under this storage scheme, multiple authorization
 codes, access tokens, and refresh tokens for a given OAuth 2.0 client and resource owner can be
 stored within a single CTS entry.",
      "propertyOrder" : 6,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
```

```
   "blacklistCacheSize" : {
     "title" : "Token Blacklist Cache Size",
     "description" : "Number of blacklisted tokens to cache in memory to speed up blacklist checks
and reduce load on the CTS.",
     "propertyOrder" : 0,
     "required" : true,
     "type" : "integer",
     "exampleValue" : ""
   },
   "blacklistPollInterval" : {
     "title" : "Blacklist Poll Interval (seconds)",
     "description" : "How frequently to poll for token blacklist changes from other servers, in
seconds.<br><br>How often each server will poll the CTS for token blacklist changes from other
servers. This is used to maintain a highly compressed view of the overall current token blacklist
improving performance. A lower number will reduce the delay for blacklisted tokens to propagate to
all servers at the cost of increased CTS load. Set to 0 to disable this feature completely.",
     "propertyOrder" : 1,
     "required" : true,
     "type" : "integer",
     "exampleValue" : ""
   },
   "jwtTokenUnreasonableLifetime" : {
     "title" : "JWT Unreasonable Lifetime (seconds)",
     "description" : "Specify the lifetime (in seconds) of a JWT which should be considered
unreasonable and rejected by validation.<br><br>The JSON Web Token (JWT) Profile for OAuth 2.0 Client
Authentication and Authorization Grants specification (https://tools.ietf.org/html/rfc7523#section-3)
states that an authorization server may reject JWTs with an \"exp\" claim value that is unreasonably
far in the future and an \"iat\" claim value that is unreasonably far in the past. During token
validation AM enforces that the token must expire within the specified duration and if the \"iat\"
claim value is present, the token must not be older than the specified duration.",
     "propertyOrder" : 8,
     "required" : true,
     "type" : "integer",
     "exampleValue" : ""
   },
   "blacklistPurgeDelay" : {
     "title" : "Blacklist Purge Delay (minutes)",
     "description" : "Length of time to blacklist tokens beyond their expiry time.<br><br>Allows
additional time to account for clock skew to ensure that a token has expired before it is removed
from the blacklist.",
     "propertyOrder" : 2,
     "required" : true,
     "type" : "integer",
     "exampleValue" : ""
   },
   "statelessGrantTokenUpgradeCompatibilityMode" : {
     "title" : "Client-Based Grant Token Upgrade Compatibility Mode",
     "description" : "Enable OpenAM to consume and create client-based OAuth 2.0 tokens in two
different formats simultaneously.<br><br>Enable this option when upgrading OpenAM to allow the new
instance to create and consume client-based OAuth 2.0 tokens in both the previous format, and the new
format. Disable this option once all OpenAM instances in the cluster have been upgraded.",
     "propertyOrder" : 5,
     "required" : true,
     "type" : "boolean",
     "exampleValue" : ""
   },
   "jwtTokenLifetimeValidationEnabled" : {
     "title" : "Enforce JWT Unreasonable Lifetime",
```

```
     "description" : "Enable the enforcement of JWT token unreasonable lifetime during
validation.<br><br>The JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and
Authorization Grants specification (https://tools.ietf.org/html/rfc7523#section-3) states that an
authorization server may reject JWTs with an \"exp\" claim value that is unreasonably far in the
future and an \"iat\" claim value that is unreasonably far in the past. This enforcement may be
disabled, but should only be done if the security implications have been evaluated.",
     "propertyOrder" : 7,
     "required" : true,
     "type" : "boolean",
     "exampleValue" : ""
   },
   "defaults" : {
     "properties" : {
       "deviceCodeConfig" : {
         "type" : "object",
         "title" : "Device Flow",
         "propertyOrder" : 5,
         "properties" : {
           "devicePollInterval" : {
             "title" : "Device Polling Interval",
             "description" : "The polling frequency for devices waiting for tokens when using the
device code flow.",
             "propertyOrder" : 400,
             "required" : true,
             "type" : "integer",
             "exampleValue" : ""
           },
           "verificationUrl" : {
             "title" : "Verification URL",
             "description" : "The URL that the user will be instructed to visit to complete their
OAuth 2.0 login and consent when using the device code flow.",
             "propertyOrder" : 370,
             "required" : false,
             "type" : "string",
             "exampleValue" : ""
           },
           "deviceCodeLifetime" : {
             "title" : "Device Code Lifetime (seconds)",
             "description" : "The lifetime of the device code, in seconds.",
             "propertyOrder" : 390,
             "required" : true,
             "type" : "integer",
             "exampleValue" : ""
           },
           "completionUrl" : {
             "title" : "Device Completion URL",
             "description" : "The URL that the user will be sent to on completion of their OAuth 2.0
login and consent when using the device code flow.",
             "propertyOrder" : 380,
             "required" : false,
             "type" : "string",
             "exampleValue" : ""
           }
         }
       },
       "coreOIDCConfig" : {
         "type" : "object",
         "title" : "OpenID Connect",
         "propertyOrder" : 3,
```

```
          "properties" : {
            "oidcDiscoveryEndpointEnabled" : {
              "title" : "OIDC Provider Discovery",
              "description" : "Turns on and off OIDC Discovery endpoint.",
              "propertyOrder" : 1000,
              "required" : true,
              "type" : "boolean",
              "exampleValue" : ""
            },
            "supportedIDTokenEncryptionAlgorithms" : {
              "title" : "ID Token Encryption Algorithms supported",
              "description" : "Encryption algorithms supported to encrypt OpenID Connect ID
 tokens in order to hide its contents.<br><br>OpenAM supports the following ID token encryption
 algorithms:<ul><li><code>RSA-OAEP</code> - RSA with Optimal Asymmetric Encryption Padding (OAEP)
 with SHA-1 and MGF-1.</li><li><code>RSA-OAEP-256</code> - RSA with OAEP with SHA-256 and MGF-1.</
li><li><code>A128KW</code> - AES Key Wrapping with 128-bit key derived from the client secret.</
li><li><code>RSA1_5</code> - RSA with PKCS#1 v1.5 padding.</li><li><code>A256KW</code> - AES
 Key Wrapping with 256-bit key derived from the client secret.</li><li><code>dir</code> - Direct
 encryption with AES using the hashed client secret.</li><li><code>A192KW</code> - AES Key Wrapping
 with 192-bit key derived from the client secret.</li></ul>",
              "propertyOrder" : 170,
              "required" : true,
              "items" : {
                "type" : "string"
              },
              "type" : "array",
              "exampleValue" : ""
            },
            "supportedClaims" : {
              "title" : "Supported Claims",
              "description" : "Set of claims supported by the OpenID Connect <code>/oauth2/
userinfo</code> endpoint, with translations.<br><br>Claims may be entered as simple strings or pipe
 separated strings representing the internal claim name, locale, and localized description.<p><p>For
 example: <code>name|en|Your full name.</code>.<p>Locale strings are in the format: <code>language
 + \"_\" + country + \"_\" + variant</code>, for example <code>en</code>, <code>en_GB</code>, or
 <code>en_US_WIN</code>. If the locale and pipe is omitted, the description is displayed to all users
 that have undefined locales.<p><p>If the description is also omitted, nothing is displayed on the
 consent page for the claim. For example specifying <code>family_name|</code> would allow the claim
 <code>family_name</code> to be used by the client, but would not display it to the user on the
 consent page when requested.",
              "propertyOrder" : 190,
              "required" : false,
              "items" : {
                "type" : "string"
              },
              "type" : "array",
              "exampleValue" : ""
            },
            "supportedIDTokenSigningAlgorithms" : {
              "title" : "ID Token Signing Algorithms supported",
              "description" : "Algorithms supported to sign OpenID Connect <code>id_tokens</
code>.<p><p>OpenAM supports signing algorithms listed in JSON Web Algorithms (JWA): <a href=\"https://
tools.ietf.org/html/rfc7518#section-3.1\">\"alg\" (Algorithm) Header Parameter Values for JWS</
a>:<ul><li><code>HS256</code> - HMAC with SHA-256.</li><li><code>HS384</code> - HMAC with SHA-384.</
li><li><code>HS512</code> - HMAC with SHA-512.</li><li><code>ES256</code> - ECDSA with SHA-256 and
 NIST standard P-256 elliptic curve.</li><li><code>ES384</code> - ECDSA with SHA-384 and NIST standard
 P-384 elliptic curve.</li><li><code>ES512</code> - ECDSA with SHA-512 and NIST standard P-521
 elliptic curve.</li><li><code>RS256</code> - RSASSA-PKCS-v1_5 using SHA-256.</li><li><code>RS384</
code> - RSASSA-PKCS-v1_5 using SHA-384.</li><li><code>RS512</code> - RSASSA-PKCS-v1_5 using SHA-512.</
```

```
li><li><code>PS256</code> - RSASSA-PSS using SHA-256.</li><li><code>PS384</code> - RSASSA-PSS using
 SHA-384.</li><li><code>PS512</code> - RSASSA-PSS using SHA-512.</li></ul>",
              "propertyOrder" : 160,
              "required" : true,
              "items" : {
                "type" : "string"
              },
              "type" : "array",
              "exampleValue" : ""
            },
            "oidcClaimsScript" : {
              "title" : "OIDC Claims Script",
              "description" : "The script that is run when issuing an ID token or making a request
 to the <i>userinfo</i> endpoint during OpenID requests.<p><p>The script gathers the scopes and
 populates claims, and has access to the access token, the user's identity and, if available, the
 user's session.",
              "propertyOrder" : 80,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            },
            "jwtTokenLifetime" : {
              "title" : "OpenID Connect JWT Token Lifetime (seconds)",
              "description" : "The amount of time the JWT will be valid for, in seconds.",
              "propertyOrder" : 210,
              "required" : true,
              "type" : "integer",
              "exampleValue" : ""
            },
            "supportedIDTokenEncryptionMethods" : {
              "title" : "ID Token Encryption Methods supported",
              "description" : "Encryption methods supported to encrypt OpenID Connect ID
 tokens in order to hide its contents.<br><br>OpenAM supports the following ID token encryption
 algorithms:<ul><li><code>A128GCM</code>, <code>A192GCM</code>, and <code>A256GCM</code> - AES
 in Galois Counter Mode (GCM) authenticated encryption mode.</li><li><code>A128CBC-HS256</code>,
 <code>A192CBC-HS384</code>, and <code>A256CBC-HS512</code> - AES encryption in CBC mode, with HMAC-
SHA-2 for integrity.</li></ul>",
              "propertyOrder" : 180,
              "required" : true,
              "items" : {
                "type" : "string"
              },
              "type" : "array",
              "exampleValue" : ""
            }
          }
        },
        "advancedOIDCConfig" : {
          "type" : "object",
          "title" : "Advanced OpenID Connect",
          "propertyOrder" : 4,
          "properties" : {
            "supportedRequestParameterEncryptionAlgorithms" : {
              "title" : "Request Parameter Encryption Algorithms Supported",
              "description" : "Encryption algorithms supported to decrypt Request
 parameter.<br><br>OpenAM supports the following ID token encryption algorithms:<ul><li><code>RSA-
OAEP</code> - RSA with Optimal Asymmetric Encryption Padding (OAEP) with SHA-1 and MGF-1.</
li><li><code>RSA-OAEP-256</code> - RSA with OAEP with SHA-256 and MGF-1.</li><li><code>A128KW</code>
 - AES Key Wrapping with 128-bit key derived from the client secret.</li><li><code>RSA1_5</code> -
```

```
RSA with PKCS#1 v1.5 padding.</li><li><code>A256KW</code> - AES Key Wrapping with 256-bit key derived
from the client secret.</li><li><code>dir</code> - Direct encryption with AES using the hashed client
secret.</li><li><code>A192KW</code> - AES Key Wrapping with 192-bit key derived from the client
secret.</li></ul>",
              "propertyOrder" : 442,
              "required" : true,
              "items" : {
                "type" : "string"
              },
              "type" : "array",
              "exampleValue" : ""
            },
            "supportedTokenEndpointAuthenticationSigningAlgorithms" : {
              "title" : "Supported Token Endpoint JWS Signing Algorithms.",
              "description" : "Supported JWS Signing Algorithms for 'private_key_jwt' JWT based
authentication method.",
              "propertyOrder" : 444,
              "required" : true,
              "items" : {
                "type" : "string"
              },
              "type" : "array",
              "exampleValue" : ""
            },
            "idTokenInfoClientAuthenticationEnabled" : {
              "title" : "Idtokeninfo Endpoint Requires Client Authentication",
              "description" : "When enabled, the <code>/oauth2/idtokeninfo</code> endpoint requires
client authentication if the signing algorithm is set to <code>HS256</code>, <code>HS384</code>, or
<code>HS512</code>.",
              "propertyOrder" : 225,
              "required" : true,
              "type" : "boolean",
              "exampleValue" : ""
            },
            "supportedRequestParameterSigningAlgorithms" : {
              "title" : "Request Parameter Signing Algorithms Supported",
              "description" : "Algorithms supported to verify signature of Request parameterOpenAM
supports signing algorithms listed in JSON Web Algorithms (JWA): <a href=\"https://
tools.ietf.org/html/rfc7518#section-3.1\">\"alg\" (Algorithm) Header Parameter Values for JWS</
a>:<ul><li><code>HS256</code> - HMAC with SHA-256.</li><li><code>HS384</code> - HMAC with SHA-384.</
li><li><code>HS512</code> - HMAC with SHA-512.</li><li><code>ES256</code> - ECDSA with SHA-256 and
NIST standard P-256 elliptic curve.</li><li><code>ES384</code> - ECDSA with SHA-384 and NIST standard
P-384 elliptic curve.</li><li><code>ES512</code> - ECDSA with SHA-512 and NIST standard P-521
elliptic curve.</li><li><code>RS256</code> - RSASSA-PKCS-v1_5 using SHA-256.</li></ul>",
              "propertyOrder" : 441,
              "required" : true,
              "items" : {
                "type" : "string"
              },
              "type" : "array",
              "exampleValue" : ""
            },
            "storeOpsTokens" : {
              "title" : "Store Ops Tokens",
              "description" : "Whether OpenAM will store the <i>ops</i> tokens corresponding to OpenID
Connect sessions in the CTS store. Note that session management related endpoints will not work when
this setting is disabled.",
              "propertyOrder" : 410,
              "required" : true,
```

```
              "type" : "boolean",
              "exampleValue" : ""
            },
            "loaMapping" : {
              "title" : "OpenID Connect acr_values to Auth Chain Mapping",
              "description" : "Maps OpenID Connect ACR values to authentication chains. For more
 details, see the <a href=\"http://openid.net/specs/openid-connect-core-1_0.html#AuthRequest\" target=
\"_blank\">acr_values parameter</a> in the OpenID Connect authentication request specification.",
              "propertyOrder" : 310,
              "required" : false,
              "patternProperties" : {
                ".*" : { }
              },
              "type" : "object",
              "exampleValue" : ""
            },
            "authorisedOpenIdConnectSSOClients" : {
              "title" : "Authorized OIDC SSO Clients",
              "description" : "Clients authorized to use OpenID Connect ID tokens as SSO
 Tokens.<br><br>Allows clients to act with the full authority of the user. Grant this permission only
 to trusted clients.",
              "propertyOrder" : 446,
              "required" : true,
              "items" : {
                "type" : "string"
              },
              "type" : "array",
              "exampleValue" : ""
            },
            "supportedUserInfoEncryptionAlgorithms" : {
              "title" : "UserInfo Encryption Algorithms Supported",
              "description" : "Encryption algorithms supported by the UserInfo endpoint.<br><br>OpenAM
 supports the following UserInfo endpoint encryption algorithms:<ul><li><code>RSA-OAEP</code> - RSA
 with Optimal Asymmetric Encryption Padding (OAEP) with SHA-1 and MGF-1.</li><li><code>RSA-OAEP-256</
code> - RSA with OAEP with SHA-256 and MGF-1.</li><li><code>A128KW</code> - AES Key Wrapping with
 128-bit key derived from the client secret.</li><li><code>RSA1_5</code> - RSA with PKCS#1 v1.5
 padding.</li><li><code>A256KW</code> - AES Key Wrapping with 256-bit key derived from the client
 secret.</li><li><code>dir</code> - Direct encryption with AES using the hashed client secret.</
li><li><code>A192KW</code> - AES Key Wrapping with 192-bit key derived from the client secret.</li></
ul>",
              "propertyOrder" : 457,
              "required" : true,
              "items" : {
                "type" : "string"
              },
              "type" : "array",
              "exampleValue" : ""
            },
            "alwaysAddClaimsToToken" : {
              "title" : "Always Return Claims in ID Tokens",
              "description" : "If enabled, include scope-derived claims in the <code>id_token</
code>, even if an access token is also returned that could provide access to get the claims from the
 <code>userinfo</code> endpoint.<br><br>If not enabled, if an access token is requested the client
 must use it to access the <code>userinfo</code> endpoint for scope-derived claims, as they will not
 be included in the ID token.",
              "propertyOrder" : 360,
              "required" : true,
              "type" : "boolean",
              "exampleValue" : ""
```

```
            },
            "amrMappings" : {
              "title" : "OpenID Connect id_token amr Values to Auth Module Mappings",
              "description" : "Specify <code>amr</code> values to be returned in the OpenID Connect
 <code>id_token</code>. Once authentication has completed, the authentication modules that were used
 from the authentication service will be mapped to the <code>amr</code> values. If you do not require
 <code>amr</code> values, or are not providing OpenID Connect tokens, leave this field blank.",
              "propertyOrder" : 330,
              "required" : false,
              "patternProperties" : {
                ".*" : { }
              },
              "type" : "object",
              "exampleValue" : ""
            },
            "jkwsURI" : {
              "title" : "Remote JSON Web Key URL",
              "description" : "The Remote URL where the providers JSON Web Key can be
 retrieved.<p><p>If this setting is not configured, then OpenAM provides a local URL to access the
 public key of the private key used to sign ID tokens.",
              "propertyOrder" : 140,
              "required" : false,
              "type" : "string",
              "exampleValue" : ""
            },
            "supportedTokenIntrospectionResponseEncryptionAlgorithms" : {
              "title" : "Token Introspection Response Encryption Algorithms Supported",
              "description" : "Encryption algorithms supported by the Token Introspection
 endpoint JWT response.<br><br>OpenAM supports the following UserInfo endpoint encryption
 algorithms:<ul><li><code>RSA-OAEP</code> - RSA with Optimal Asymmetric Encryption Padding (OAEP)
 with SHA-1 and MGF-1.</li><li><code>RSA-OAEP-256</code> - RSA with OAEP with SHA-256 and MGF-1.</
li><li><code>A128KW</code> - AES Key Wrapping with 128-bit key derived from the client secret.</
li><li><code>RSA1_5</code> - RSA with PKCS#1 v1.5 padding.</li><li><code>A256KW</code> - AES
 Key Wrapping with 256-bit key derived from the client secret.</li><li><code>dir</code> - Direct
 encryption with AES using the hashed client secret.</li><li><code>A192KW</code> - AES Key Wrapping
 with 192-bit key derived from the client secret.</li></ul>",
              "propertyOrder" : 460,
              "required" : true,
              "items" : {
                "type" : "string"
              },
              "type" : "array",
              "exampleValue" : ""
            },
            "claimsParameterSupported" : {
              "title" : "Enable \"claims_parameter_supported\"",
              "description" : "If enabled, clients will be able to request individual claims using
 the <code>claims</code> request parameter, as per <a href=\"http://openid.net/specs/openid-connect-
core-1_0.html#ClaimsParameter\" target=\"_blank\">section 5.5 of the OpenID Connect specification</
a>.",
              "propertyOrder" : 250,
              "required" : true,
              "type" : "boolean",
              "exampleValue" : ""
            },
            "supportedUserInfoSigningAlgorithms" : {
              "title" : "UserInfo Signing Algorithms Supported",
              "description" : "Algorithms supported to verify signature of the UserInfo endpoint.
 OpenAM supports signing algorithms listed in JSON Web Algorithms (JWA): <a href=\"https://
```

```
tools.ietf.org/html/rfc7518#section-3.1\">\"alg\" (Algorithm) Header Parameter Values for JWS</
a>:<ul><li><code>HS256</code> - HMAC with SHA-256.</li><li><code>HS384</code> - HMAC with SHA-384.</
li><li><code>HS512</code> - HMAC with SHA-512.</li><li><code>ES256</code> - ECDSA with SHA-256 and
 NIST standard P-256 elliptic curve.</li><li><code>ES384</code> - ECDSA with SHA-384 and NIST standard
 P-384 elliptic curve.</li><li><code>ES512</code> - ECDSA with SHA-512 and NIST standard P-521
 elliptic curve.</li><li><code>RS256</code> - RSASSA-PKCS-v1_5 using SHA-256.</li></ul>",
              "propertyOrder" : 456,
              "required" : true,
              "items" : {
                "type" : "string"
              },
              "type" : "array",
              "exampleValue" : ""
            },
            "supportedTokenIntrospectionResponseEncryptionEnc" : {
              "title" : "Token Introspection Response Encryption Methods Supported",
              "description" : "Encryption methods supported by the Token Introspection endpoint JWT
 response.<br><br>OpenAM supports the following encryption methods:<ul><li><code>A128GCM</code>,
 <code>A192GCM</code>, and <code>A256GCM</code> - AES in Galois Counter Mode (GCM) authenticated
 encryption mode.</li><li><code>A128CBC-HS256</code>, <code>A192CBC-HS384</code>, and <code>A256CBC-
HS512</code> - AES encryption in CBC mode, with HMAC-SHA-2 for integrity.</li></ul>",
              "propertyOrder" : 461,
              "required" : true,
              "items" : {
                "type" : "string"
              },
              "type" : "array",
              "exampleValue" : ""
            },
            "supportedTokenIntrospectionResponseSigningAlgorithms" : {
              "title" : "Token Introspection Response Signing Algorithms Supported",
              "description" : "Algorithms that are supported for signing the Token Introspection
 endpoint JWT response.<br><br>OpenAM supports signing algorithms listed in JSON Web Algorithms (JWA):
 <a href=\"https://tools.ietf.org/html/rfc7518#section-3.1\">\"alg\" (Algorithm) Header Parameter
 Values for JWS</a>:<ul><li><code>HS256</code> - HMAC with SHA-256.</li><li><code>HS384</code> -
 HMAC with SHA-384.</li><li><code>HS512</code> - HMAC with SHA-512.</li><li><code>ES256</code> -
 ECDSA with SHA-256 and NIST standard P-256 elliptic curve.</li><li><code>ES384</code> - ECDSA with
 SHA-384 and NIST standard P-384 elliptic curve.</li><li><code>ES512</code> - ECDSA with SHA-512 and
 NIST standard P-521 elliptic curve.</li><li><code>RS256</code> - RSASSA-PKCS-v1_5 using SHA-256.</
li><li><code>RS384</code> - RSASSA-PKCS-v1_5 using SHA-384.</li><li><code>RS512</code> - RSASSA-PKCS-
v1_5 using SHA-512.</li><li><code>EdDSA</code> - EdDSA with SHA-512.</li></ul>",
              "propertyOrder" : 459,
              "required" : true,
              "items" : {
                "type" : "string"
              },
              "type" : "array",
              "exampleValue" : ""
            },
            "includeAllKtyAlgCombinationsInJwksUri" : {
              "title" : "Include all kty and alg combinations in jwks_uri",
              "description" : "By default only distinct kid entries are returned in the jwks_uri
 and the alg property is not included.Enabling this flag will result in duplicate kid entries,
 each one specifying a different kty and alg combination. <a href=\"https://tools.ietf.org/html/
rfc7517#section-4.5\">RFC7517 distinct key KIDs</a>",
              "propertyOrder" : 630,
              "required" : true,
              "type" : "boolean",
              "exampleValue" : ""
```

```
            },
            "defaultACR" : {
              "title" : "Default ACR values",
              "description" : "Default requested Authentication Context Class Reference
 values.<br><br>List of strings that specifies the default acr values that the OP is being requested
 to use for processing requests from this Client, with the values appearing in order of preference.
 The Authentication Context Class satisfied by the authentication performed is returned as the
 acr Claim Value in the issued ID Token. The acr Claim is requested as a Voluntary Claim by this
 parameter. The acr_values_supported discovery element contains a list of the acr values supported by
 this server. Values specified in the acr_values request parameter or an individual acr Claim request
 override these default values.",
              "propertyOrder" : 320,
              "required" : false,
              "items" : {
                "type" : "string"
              },
              "type" : "array",
              "exampleValue" : ""
            },
            "supportedUserInfoEncryptionEnc" : {
              "title" : "UserInfo Encryption Methods Supported",
              "description" : "Encryption methods supported by the UserInfo endpoint.<br><br>OpenAM
 supports the following UserInfo endpoint encryption methods:<ul><li><code>A128GCM</code>,
 <code>A192GCM</code>, and <code>A256GCM</code> - AES in Galois Counter Mode (GCM) authenticated
 encryption mode.</li><li><code>A128CBC-HS256</code>, <code>A192CBC-HS384</code>, and <code>A256CBC-
HS512</code> - AES encryption in CBC mode, with HMAC-SHA-2 for integrity.</li></ul>",
              "propertyOrder" : 458,
              "required" : true,
              "items" : {
                "type" : "string"
              },
              "type" : "array",
              "exampleValue" : ""
            },
            "supportedRequestParameterEncryptionEnc" : {
              "title" : "Request Parameter Encryption Methods Supported",
              "description" : "Encryption methods supported to decrypt Request
 parameter.<br><br>OpenAM supports the following Request parameter encryption
 algorithms:<ul><li><code>A128GCM</code>, <code>A192GCM</code>, and <code>A256GCM</code> - AES
 in Galois Counter Mode (GCM) authenticated encryption mode.</li><li><code>A128CBC-HS256</code>,
 <code>A192CBC-HS384</code>, and <code>A256CBC-HS512</code> - AES encryption in CBC mode, with HMAC-
SHA-2 for integrity.</li></ul>",
              "propertyOrder" : 443,
              "required" : true,
              "items" : {
                "type" : "string"
              },
              "type" : "array",
              "exampleValue" : ""
            }
          }
        },
        "clientDynamicRegistrationConfig" : {
          "type" : "object",
          "title" : "Client Dynamic Registration",
          "propertyOrder" : 2,
          "properties" : {
            "generateRegistrationAccessTokens" : {
              "title" : "Generate Registration Access Tokens",
```

```
              "description" : "Whether to generate Registration Access Tokens for clients that
 register by using open dynamic client registration. Such tokens allow the client to access the <a
 href=\"https://openid.net/specs/openid-connect-registration-1_0.html#ClientConfigurationEndpoint\"
 target=\"_blank\">Client Configuration Endpoint</a> as per the OpenID Connect specification. This
 setting has no effect if Allow Open Dynamic Client Registration is disabled.",
              "propertyOrder" : 290,
              "required" : true,
              "type" : "boolean",
              "exampleValue" : ""
            },
            "dynamicClientRegistrationScope" : {
              "title" : "Scope to give access to dynamic client registration",
              "description" : "Mandatory scope required when registering a new OAuth2 client.",
              "propertyOrder" : 455,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            },
            "dynamicClientRegistrationSoftwareStatementRequired" : {
              "title" : "Require Software Statement for Dynamic Client Registration",
              "description" : "When enabled, a software statement JWT containing at least the
 <code>iss</code> (issuer) claim must be provided when registering an OAuth 2.0 client dynamically.",
              "propertyOrder" : 271,
              "required" : true,
              "type" : "boolean",
              "exampleValue" : ""
            },
            "allowDynamicRegistration" : {
              "title" : "Allow Open Dynamic Client Registration",
              "description" : "Allow clients to register without an access token. If enabled, you
 should consider adding some form of rate limiting. For more information, see  <a href=\"https://
openid.net/specs/openid-connect-registration-1_0.html#ClientRegistration\" target=\"_blank\">Client
 Registration</a> in the OpenID Connect specification.",
              "propertyOrder" : 280,
              "required" : true,
              "type" : "boolean",
              "exampleValue" : ""
            },
            "requiredSoftwareStatementAttestedAttributes" : {
              "title" : "Required Software Statement Attested Attributes",
              "description" : "The client attributes that are required to be present in the software
 statement JWT when registering an OAuth 2.0 client dynamically. Only applies if Require Software
 Statements for Dynamic Client Registration is enabled.<br><br>Leave blank to allow any attributes to
 be present.",
              "propertyOrder" : 272,
              "required" : true,
              "items" : {
                "type" : "string"
              },
              "type" : "array",
              "exampleValue" : ""
            }
          }
        },
        "advancedOAuth2Config" : {
          "type" : "object",
          "title" : "Advanced",
          "propertyOrder" : 1,
          "properties" : {
```

```
            "hashSalt" : {
              "title" : "Subject Identifier Hash Salt",
              "description" : "If <i>pairwise</i> subject types are supported, it is <em>STRONGLY
 RECOMMENDED</em> to change this value. It is used in the salting of hashes for returning
 specific <code>sub</code> claims to individuals using the same <code>request_uri</code> or
 <code>sector_identifier_uri</code>.",
              "propertyOrder" : 260,
              "required" : false,
              "type" : "string",
              "exampleValue" : ""
            },
            "tlsClientCertificateHeaderFormat" : {
              "title" : "TLS Client Certificate Header Format",
              "description" : "Format of the HTTP header used to communicate a client certificate
 from a reverse proxy.<br><br>The following formats are supported:<ul><li><code>URLENCODED_PEM</
code> - a URL-encoded PEM format certificate. This is the format used by Nginx.</
li><li><code>X_FORWARDED_CLIENT_CERT</code> - the <a target=\"_blank\" href=\"https://
www.envoyproxy.io/docs/envoy/latest/configuration/http/http_conn_man/headers#config-http-conn-man-
headers-x-forwarded-client-cert\">X-Forwarded-Client-Cert</a>format used by Envoy and Istio.</li></
ul>",
              "propertyOrder" : 605,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            },
            "grantTypes" : {
              "title" : "Grant Types",
              "description" : "The set of Grant Types (OAuth2 Flows) that are permitted to be used by
 this client.<br><br>If no Grant Types (OAuth2 Flows) are configured nothing will be permitted.",
              "propertyOrder" : 560,
              "required" : true,
              "items" : {
                "type" : "string"
              },
              "type" : "array",
              "exampleValue" : ""
            },
            "scopeImplementationClass" : {
              "title" : "Scope Implementation Class",
              "description" : "The class that contains the required scope implementation, must
 implement the <code>org.forgerock.oauth2.core.ScopeValidator</code> interface.",
              "propertyOrder" : 70,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            },
            "passwordGrantAuthService" : {
              "title" : "Password Grant Authentication Service",
              "description" : "The authentication service (chain or tree) that will be used to
 authenticate the username and password for the resource owner password credentials grant type.",
              "propertyOrder" : 430,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            },
            "supportedScopes" : {
              "title" : "Client Registration Scope Whitelist",
              "description" : "The set of scopes allowed when registering clients dynamically,
 with translations.<br><br><p>Scopes may be entered as simple strings or pipe-separated strings
```

```
 representing the internal scope name, locale, and localized description.</p><p>For example:
 <code>read|en|Permission to view email messages in your account</code></p><p>Locale strings are in
 the format: <code>language_country_variant</code>, for example <code>en</code>, <code>en_GB</code>,
 or <code>en_US_WIN</code>.</p><p>If the locale and pipe is omitted, the description is displayed
 to all users that have undefined locales.</p><p>If the description is also omitted, nothing is
 displayed on the consent page for the scope. For example specifying <code>read|</code> would allow
 the scope read to be used by the client, but would not display it to the user on the consent page
 when requested.</p>",
              "propertyOrder" : 130,
              "required" : true,
              "items" : {
                "type" : "string"
              },
              "type" : "array",
              "exampleValue" : ""
            },
            "modifiedTimestampAttribute" : {
              "title" : "Modified Timestamp Attribute Name",
              "description" : "The identity Data Store attribute used to return modified timestamp
 values.<p>This attribute is paired together with the <em>Created Timestamp Attribute Name</em>
 attribute (<code>createdTimestampAttribute</code>). You can leave both attributes unset (default) or
 set them both. If you set only one attribute and leave the other blank, the access token fails with
 a 500 error.<p>For example, when you configure AM as an OpenID Connect Provider in a Mobile Connect
 application and use DS as an identity data store, the client accesses the <code>userinfo</code>
 endpoint to obtain the <code>updated_at</code> claim value in the ID token. The <code>updated_at</
code> claim obtains its value from the <code>modifiedTimestampAttribute</code> attribute in the
 user profile. If the profile has never been modified the <code>updated_at</code> claim uses the
 <code>createdTimestampAttribute</code> attribute. ",
              "propertyOrder" : 340,
              "required" : false,
              "type" : "string",
              "exampleValue" : ""
            },
            "createdTimestampAttribute" : {
              "title" : "Created Timestamp Attribute Name",
              "description" : "The identity Data Store attribute used to return created timestamp
 values.",
              "propertyOrder" : 350,
              "required" : false,
              "type" : "string",
              "exampleValue" : ""
            },
            "supportedSubjectTypes" : {
              "title" : "Subject Types supported",
              "description" : "List of subject types supported. Valid values
 are:<ul><li><code>public</code> - Each client receives the same subject (<code>sub</code>) value.</
li><li><code>pairwise</code> - Each client receives a different subject (<code>sub</code>) value, to
 prevent correlation between clients.</li></ul>",
              "propertyOrder" : 150,
              "required" : true,
              "items" : {
                "type" : "string"
              },
              "type" : "array",
              "exampleValue" : ""
            },
            "allowedAudienceValues" : {
              "title" : "Additional Audience Values",
```

```
            "description" : "The additional audience values that will be permitted when verifying
Client Authentication JWTs.<br><br>These audience values will be in addition to the AS base, issuer
and endpoint URIs.",
            "propertyOrder" : 91,
            "required" : false,
            "items" : {
              "type" : "string"
            },
            "type" : "array",
            "exampleValue" : ""
          },
          "tlsCertificateRevocationCheckingEnabled" : {
            "title" : "Check TLS Certificate Revocation Status",
            "description" : "Whether to check if TLS client certificates have been
revoked.<br><br>If enabled then AM will check if TLS client certificates used for client
authentication have been revoked using either OCSP (preferred) or CRL. AM implements \"soft fail\"
semantics: if the revocation status cannot be established due to a temporary error (e.g., network
error) then the certificate is assumed to still be valid.",
            "propertyOrder" : 615,
            "required" : true,
            "type" : "boolean",
            "exampleValue" : ""
          },
          "displayNameAttribute" : {
            "title" : "User Display Name attribute",
            "description" : "The profile attribute that contains the name to be displayed for the
user on the consent page.",
            "propertyOrder" : 120,
            "required" : true,
            "type" : "string",
            "exampleValue" : ""
          },
          "tlsOcspResponderUri" : {
            "title" : "OCSP Responder URI",
            "description" : "URI of the OCSP responder service to use for checking certificate
revocation status.<br><br>If specified this value overrides any OCSP or CRL mechanisms specified in
individual certificates.",
            "propertyOrder" : 616,
            "required" : false,
            "type" : "string",
            "exampleValue" : ""
          },
          "tokenCompressionEnabled" : {
            "title" : "Client-Based Token Compression",
            "description" : "Whether client-based access and refresh tokens should be compressed.",
            "propertyOrder" : 223,
            "required" : true,
            "type" : "boolean",
            "exampleValue" : ""
          },
          "tokenEncryptionEnabled" : {
            "title" : "Encrypt Client-Based Tokens",
            "description" : "Whether client-based access and refresh tokens should be
encrypted.<br><br>Enabling token encryption will disable token signing as encryption is performed
using direct symmetric encryption.",
            "propertyOrder" : 242,
            "required" : true,
            "type" : "boolean",
            "exampleValue" : ""
```

```
            },
            "tlsOcspResponderCert" : {
              "title" : "OCSP Responder Certificate",
              "description" : "PEM-encoded certificate to use to verify OCSP responses.<br><br>If
 specified this certificate will be used to verify the signature on all OCSP responses. Otherwise the
 appropriate certificate will be determined from the trusted CA certificates.",
              "propertyOrder" : 617,
              "required" : false,
              "type" : "string",
              "exampleValue" : ""
            },
            "tokenSigningAlgorithm" : {
              "title" : "OAuth2 Token Signing Algorithm",
              "description" : "Algorithm used to sign client-based OAuth 2.0 tokens in order to
 detect tampering.<br><br>OpenAM supports signing algorithms listed in JSON Web Algorithms (JWA): <a
 href=\"https://tools.ietf.org/html/rfc7518#section-3.1\">\"alg\" (Algorithm) Header Parameter Values
 for JWS</a>:<ul><li><code>HS256</code> - HMAC with SHA-256.</li><li><code>HS384</code> - HMAC with
 SHA-384.</li><li><code>HS512</code> - HMAC with SHA-512.</li><li><code>ES256</code> - ECDSA with
 SHA-256 and NIST standard P-256 elliptic curve.</li><li><code>ES384</code> - ECDSA with SHA-384 and
 NIST standard P-384 elliptic curve.</li><li><code>ES512</code> - ECDSA with SHA-512 and NIST standard
 P-521 elliptic curve.</li><li><code>RS256</code> - RSASSA-PKCS-v1_5 using SHA-256.</li></ul>",
              "propertyOrder" : 220,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            },
            "customLoginUrlTemplate" : {
              "title" : "Custom Login URL Template",
              "description" : "Custom URL for handling login, to override the default OpenAM login
 page.<br><br>Supports Freemarker syntax, with the following variables:<table><tr><th>Variable</
th><th>Description</th></tr><tr><td><code>gotoUrl</code></td><td><p>The URL to redirect to after
 login.</p></td></tr><tr><td><code>acrValues</code></td><td><p>The Authentication Context Class
 Reference (acr) values for the authorization request.</p></td></tr><tr><td><code>realm</code></
td><td><p>The OpenAM realm the authorization request was made on.</p></td></tr><tr><td><code>module</
code></td><td><p>The name of the OpenAM authentication module requested to perform resource
 owner authentication.</p></td></tr><tr><td><code>service</code></td><td><p>The name of the
 OpenAM authentication chain requested to perform resource owner authentication.</p></td></
tr><tr><td><code>locale</code></td><td><p>A space-separated list of locales, ordered by
 preference.</p></td></tr></table>The following example template redirects users to a non-OpenAM
 front end to handle login, which will then redirect back to the <code>/oauth2/authorize</code>
 endpoint with any required parameters:<p> <code>http://mylogin.com/login?goto=${goto}&lt;#if
 acrValues??&gt;&amp;acr_values=${acrValues}&lt;&#x2F;#if&gt;&lt;#if realm??&gt;&amp;realm=
${realm}&lt;&#x2F;#if&gt;&lt;#if module??&gt;&amp;module=${module}&lt;&#x2F;#if&gt;&lt;#if
 service??&gt;&amp;service=${service}&lt;&#x2F;#if&gt;&lt;#if locale??&gt;&amp;locale=
${locale}&lt;&#x2F;#if&gt;</code><br><b>NOTE</b>: Default OpenAM login page is constructed using
 \"Base URL Source\" service.",
              "propertyOrder" : 60,
              "required" : false,
              "type" : "string",
              "exampleValue" : ""
            },
            "moduleMessageEnabledInPasswordGrant" : {
              "title" : "Enable Auth Module Messages for Password Credentials Grant",
              "description" : "If enabled, authentication module failure messages are used to create
 Resource Owner Password Credentials Grant failure messages. If disabled, a standard authentication
 failed message is used.<br><br>The Password Grant Type requires the <code>grant_type=password</code>
 parameter.",
              "propertyOrder" : 440,
              "required" : true,
```

```
              "type" : "boolean",
              "exampleValue" : ""
            },
            "tlsClientCertificateTrustedHeader" : {
              "title" : "Trusted TLS Client Certificate Header",
              "description" : "HTTP Header to receive TLS client certificates when TLS is terminated
 at a proxy.<br><br>Leave blank if not terminating TLS at a proxy. Ensure that the proxy is configured
 to strip this headerfrom incoming requests. Best practice is to use a random string.",
              "propertyOrder" : 600,
              "required" : false,
              "type" : "string",
              "exampleValue" : ""
            },
            "defaultScopes" : {
              "title" : "Default Client Scopes",
              "description" : "List of scopes a client will be granted if they request registration
 without specifying which scopes they want. Default scopes are NOT auto-granted to clients created
 through the OpenAM console.",
              "propertyOrder" : 200,
              "required" : false,
              "items" : {
                "type" : "string"
              },
              "type" : "array",
              "exampleValue" : ""
            },
            "codeVerifierEnforced" : {
              "title" : "Code Verifier Parameter Required",
              "description" : "If enabled, requests using the authorization code grant require a
 <code>code_challenge</code> attribute.<br><br>For more information, read the <a href=\"https://
tools.ietf.org/html/rfc7636\">specification for this feature</a>.",
              "propertyOrder" : 270,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            },
            "macaroonTokenFormat" : {
              "title" : "Macaroon Token Format",
              "description" : "The format to use when serializing and parsing Macaroons. V1 is bulky
 and should only be used when compatibility with older Macaroon libraries is required.",
              "propertyOrder" : 620,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            },
            "authenticationAttributes" : {
              "title" : "User Profile Attribute(s) the Resource Owner is Authenticated On",
              "description" : "Names of profile attributes that resource owners use to log in. You can
 add others to the default, for example <code>mail</code>.",
              "propertyOrder" : 100,
              "required" : true,
              "items" : {
                "type" : "string"
              },
              "type" : "array",
              "exampleValue" : ""
            },
            "responseTypeClasses" : {
              "title" : "Response Type Plugins",
```

```
              "description" : "List of plugins that handle the valid <code>response_type</code>
 values.<br><br>OAuth 2.0 clients pass response types as parameters to the OAuth 2.0 Authorization
 endpoint (<code>/oauth2/authorize</code>) to indicate which grant type is requested from the
 provider. For example, the client passes <code>code</code> when requesting an authorization code,
 and <code>token</code> when requesting an access token.<p><p>Values in this list take the form
 <code>response-type|plugin-class-name</code>.",
              "propertyOrder" : 90,
              "required" : true,
              "items" : {
                "type" : "string"
              },
              "type" : "array",
              "exampleValue" : ""
            },
            "tlsCertificateBoundAccessTokensEnabled" : {
              "title" : "Support TLS Certificate-Bound Access Tokens",
              "description" : "Whether to bind access tokens to the client certificate when using TLS
 client certificate authentication.",
              "propertyOrder" : 610,
              "required" : true,
              "type" : "boolean",
              "exampleValue" : ""
            }
          }
        },
        "consent" : {
          "type" : "object",
          "title" : "Consent",
          "propertyOrder" : 6,
          "properties" : {
            "supportedRcsRequestEncryptionMethods" : {
              "title" : "Remote Consent Service Request Encryption Methods Supported",
              "description" : "Encryption methods supported to encrypt Remote Consent Service
 requests.<br><br>OpenAM supports the following encryption methods:<ul><li><code>A128GCM</code>,
 <code>A192GCM</code>, and <code>A256GCM</code> - AES in Galois Counter Mode (GCM) authenticated
 encryption mode.</li><li><code>A128CBC-HS256</code>, <code>A192CBC-HS384</code>, and <code>A256CBC-
HS512</code> - AES encryption in CBC mode, with HMAC-SHA-2 for integrity.</li></ul>",
              "propertyOrder" : 451,
              "required" : true,
              "items" : {
                "type" : "string"
              },
              "type" : "array",
              "exampleValue" : ""
            },
            "enableRemoteConsent" : {
              "title" : "Enable Remote Consent",
              "description" : "",
              "propertyOrder" : 447,
              "required" : true,
              "type" : "boolean",
              "exampleValue" : ""
            },
            "savedConsentAttribute" : {
              "title" : "Saved Consent Attribute Name",
              "description" : "Name of a multi-valued attribute on resource owner profiles where
 OpenAM can save authorization consent decisions.<p><p>When the resource owner chooses to save the
 decision to authorize access for a client application, then OpenAM updates the resource owner's
```

```
 profile to avoid having to prompt the resource owner to grant authorization when the client issues
 subsequent authorization requests.",
              "propertyOrder" : 110,
              "required" : false,
              "type" : "string",
              "exampleValue" : ""
            },
            "supportedRcsResponseSigningAlgorithms" : {
              "title" : "Remote Consent Service Response Signing Algorithms Supported",
              "description" : "Algorithms supported to verify signed consent_response JWT from Remote
 Consent Services.<br><br>OpenAM supports signing algorithms listed in JSON Web Algorithms (JWA): <a
 href=\"https://tools.ietf.org/html/rfc7518#section-3.1\">\"alg\" (Algorithm) Header Parameter Values
 for JWS</a>:<ul><li><code>HS256</code> - HMAC with SHA-256.</li><li><code>HS384</code> - HMAC with
 SHA-384.</li><li><code>HS512</code> - HMAC with SHA-512.</li><li><code>ES256</code> - ECDSA with
 SHA-256 and NIST standard P-256 elliptic curve.</li><li><code>ES384</code> - ECDSA with SHA-384 and
 NIST standard P-384 elliptic curve.</li><li><code>ES512</code> - ECDSA with SHA-512 and NIST standard
 P-521 elliptic curve.</li><li><code>RS256</code> - RSASSA-PKCS-v1_5 using SHA-256.</li></ul>",
              "propertyOrder" : 452,
              "required" : true,
              "items" : {
                "type" : "string"
              },
              "type" : "array",
              "exampleValue" : ""
            },
            "remoteConsentServiceId" : {
              "title" : "Remote Consent Service ID",
              "description" : "The ID of an existing remote consent service agent.",
              "propertyOrder" : 448,
              "required" : false,
              "type" : "string",
              "exampleValue" : ""
            },
            "clientsCanSkipConsent" : {
              "title" : "Allow Clients to Skip Consent",
              "description" : "If enabled, clients may be configured so that the resource owner will
 not be asked for consent during authorization flows.",
              "propertyOrder" : 420,
              "required" : true,
              "type" : "boolean",
              "exampleValue" : ""
            },
            "supportedRcsRequestSigningAlgorithms" : {
              "title" : "Remote Consent Service Request Signing Algorithms Supported",
              "description" : "Algorithms supported to sign consent_request JWTs for Remote Consent
 Services.<br><br>OpenAM supports signing algorithms listed in JSON Web Algorithms (JWA): <a href=
\"https://tools.ietf.org/html/rfc7518#section-3.1\">\"alg\" (Algorithm) Header Parameter Values for
 JWS</a>:<ul><li><code>HS256</code> - HMAC with SHA-256.</li><li><code>HS384</code> - HMAC with
 SHA-384.</li><li><code>HS512</code> - HMAC with SHA-512.</li><li><code>ES256</code> - ECDSA with
 SHA-256 and NIST standard P-256 elliptic curve.</li><li><code>ES384</code> - ECDSA with SHA-384 and
 NIST standard P-384 elliptic curve.</li><li><code>ES512</code> - ECDSA with SHA-512 and NIST standard
 P-521 elliptic curve.</li><li><code>RS256</code> - RSASSA-PKCS-v1_5 using SHA-256.</li></ul>",
              "propertyOrder" : 449,
              "required" : true,
              "items" : {
                "type" : "string"
              },
              "type" : "array",
              "exampleValue" : ""
```

```
            },
            "supportedRcsResponseEncryptionAlgorithms" : {
              "title" : "Remote Consent Service Response Encryption Algorithms Supported",
              "description" : "Encryption algorithms supported to decrypt Remote Consent Service
 responses.<br><br>OpenAM supports the following encryption algorithms:<ul><li><code>RSA1_5</code> -
 RSA with PKCS#1 v1.5 padding.</li><li><code>RSA-OAEP</code> - RSA with Optimal Asymmetric Encryption
 Padding (OAEP) with SHA-1 and MGF-1.</li><li><code>RSA-OAEP-256</code> - RSA with OAEP with SHA-256
 and MGF-1.</li><li><code>A128KW</code> - AES Key Wrapping with 128-bit key derived from the client
 secret.</li><li><code>A192KW</code> - AES Key Wrapping with 192-bit key derived from the client
 secret.</li><li><code>A256KW</code> - AES Key Wrapping with 256-bit key derived from the client
 secret.</li><li><code>dir</code> - Direct encryption with AES using the hashed client secret.</li></
ul>",
              "propertyOrder" : 453,
              "required" : true,
              "items" : {
                "type" : "string"
              },
              "type" : "array",
              "exampleValue" : ""
            },
            "supportedRcsResponseEncryptionMethods" : {
              "title" : "Remote Consent Service Response Encryption Methods Supported",
              "description" : "Encryption methods supported to decrypt Remote Consent Service
 responses.<br><br>OpenAM supports the following encryption methods:<ul><li><code>A128GCM</code>,
 <code>A192GCM</code>, and <code>A256GCM</code> - AES in Galois Counter Mode (GCM) authenticated
 encryption mode.</li><li><code>A128CBC-HS256</code>, <code>A192CBC-HS384</code>, and <code>A256CBC-
HS512</code> - AES encryption in CBC mode, with HMAC-SHA-2 for integrity.</li></ul>",
              "propertyOrder" : 454,
              "required" : true,
              "items" : {
                "type" : "string"
              },
              "type" : "array",
              "exampleValue" : ""
            },
            "supportedRcsRequestEncryptionAlgorithms" : {
              "title" : "Remote Consent Service Request Encryption Algorithms Supported",
              "description" : "Encryption algorithms supported to encrypt Remote Consent Service
 requests.<br><br>OpenAM supports the following encryption algorithms:<ul><li><code>RSA1_5</code> -
 RSA with PKCS#1 v1.5 padding.</li><li><code>RSA-OAEP</code> - RSA with Optimal Asymmetric Encryption
 Padding (OAEP) with SHA-1 and MGF-1.</li><li><code>RSA-OAEP-256</code> - RSA with OAEP with SHA-256
 and MGF-1.</li><li><code>A128KW</code> - AES Key Wrapping with 128-bit key derived from the client
 secret.</li><li><code>A192KW</code> - AES Key Wrapping with 192-bit key derived from the client
 secret.</li><li><code>A256KW</code> - AES Key Wrapping with 256-bit key derived from the client
 secret.</li><li><code>dir</code> - Direct encryption with AES using the hashed client secret.</li></
ul>",
              "propertyOrder" : 450,
              "required" : true,
              "items" : {
                "type" : "string"
              },
              "type" : "array",
              "exampleValue" : ""
            }
          }
        },
        "coreOAuth2Config" : {
          "type" : "object",
          "title" : "Core",
```

```
          "propertyOrder" : 0,
          "properties" : {
            "codeLifetime" : {
              "title" : "Authorization Code Lifetime (seconds)",
              "description" : "The time an authorization code is valid for, in seconds.",
              "propertyOrder" : 10,
              "required" : true,
              "type" : "integer",
              "exampleValue" : ""
            },
            "usePolicyEngineForScope" : {
              "title" : "Use Policy Engine for Scope decisions",
              "description" : "With this setting enabled, the policy engine is consulted for each
scope value that is requested.<br><br>If a policy returns an action of GRANT=true, the scope is
consented automatically, and the user is not consulted in a user-interaction flow. If a policy
returns an action of GRANT=false, the scope is not added to any resulting token, and the user will
not see it in a user-interaction flow. If no policy returns a value for the GRANT action, then
if the grant type is user-facing (i.e. authorization or device code flows), the user is asked for
consent (or saved consent is used), and if the grant type is not user-facing (password or client
credentials), the scope is not added to any resulting token.",
              "propertyOrder" : 55,
              "required" : true,
              "type" : "boolean",
              "exampleValue" : ""
            },
            "issueRefreshTokenOnRefreshedToken" : {
              "title" : "Issue Refresh Tokens on Refreshing Access Tokens",
              "description" : "Whether to issue a refresh token when refreshing an access token.",
              "propertyOrder" : 50,
              "required" : true,
              "type" : "boolean",
              "exampleValue" : ""
            },
            "accessTokenLifetime" : {
              "title" : "Access Token Lifetime (seconds)",
              "description" : "The time an access token is valid for, in seconds. Note that if you set
the value to <code>0</code>, the access token will not be valid. A maximum lifetime of 600 seconds is
recommended.",
              "propertyOrder" : 30,
              "required" : true,
              "type" : "integer",
              "exampleValue" : ""
            },
            "refreshTokenLifetime" : {
              "title" : "Refresh Token Lifetime (seconds)",
              "description" : "The time in seconds a refresh token is valid for. If this field is set
to <code>-1</code>, the refresh token will never expire.",
              "propertyOrder" : 20,
              "required" : true,
              "type" : "integer",
              "exampleValue" : ""
            },
            "macaroonTokensEnabled" : {
              "title" : "Use Macaroon Access and Refresh Tokens",
              "description" : "When enabled, AM will issue access and refresh tokens as Macaroons with
caveats.",
              "propertyOrder" : 6,
              "required" : true,
              "type" : "boolean",
```

```
              "exampleValue" : ""
            },
            "issueRefreshToken" : {
              "title" : "Issue Refresh Tokens",
              "description" : "Whether to issue a refresh token when returning an access token.",
              "propertyOrder" : 40,
              "required" : true,
              "type" : "boolean",
              "exampleValue" : ""
            },
            "accessTokenModificationScript" : {
              "title" : "OAuth2 Access Token Modification Script",
              "description" : "The script that is executed when issuing an access token. The script
 can change the access token's internal data structure to include or exclude particular fields.",
              "propertyOrder" : 75,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            },
            "statelessTokensEnabled" : {
              "title" : "Use Client-Based Access & Refresh Tokens",
              "description" : "When enabled, OpenAM issues access and refresh tokens that can be
 inspected by resource servers.",
              "propertyOrder" : 3,
              "required" : true,
              "type" : "boolean",
              "exampleValue" : ""
            }
          }
        },
        "cibaConfig" : {
          "type" : "object",
          "title" : "CIBA",
          "propertyOrder" : 7,
          "properties" : {
            "cibaAuthReqIdLifetime" : {
              "title" : "Back Channel Authentication ID Lifetime (seconds)",
              "description" : "The time back channel authentication request id is valid for, in
 seconds.",
              "propertyOrder" : 700,
              "required" : true,
              "type" : "integer",
              "exampleValue" : ""
            },
            "cibaMinimumPollingInterval" : {
              "title" : "Polling Wait Interval (seconds)",
              "description" : "The minimum amount of time in seconds that the Client should wait
 between polling requests to the token endpoint",
              "propertyOrder" : 800,
              "required" : true,
              "type" : "integer",
              "exampleValue" : ""
            },
            "supportedCibaSigningAlgorithms" : {
              "title" : "Signing Algorithms Supported",
              "description" : "Algorithms supported to sign the CIBA request parameter.<p><p>OpenAM
 supports signing algorithms listed in JSON Web Algorithms (JWA): <a href=\"https://
tools.ietf.org/html/rfc7518#section-3.1\">\"alg\" (Algorithm) Header Parameter Values for JWS</
```

```
a>:<ul><li><code>ES256</code> - ECDSA with SHA-256 and NIST standard P-256 elliptic curve.</
li><li><code>PS256</code> - RSASSA-PSS using SHA-256.</li></ul>",
              "propertyOrder" : 900,
              "required" : true,
              "items" : {
                "type" : "string"
              },
              "type" : "array",
              "exampleValue" : ""
            }
          }
        }
      },
      "type" : "object",
      "title" : "Realm Defaults"
    }
  }
}
```

OAuth2RemoteConsentAgentGroups

Realm Operations

Agent Groups handler that is responsible for managing agent groups

Resource path: `/realm-config/agents/groups/RemoteConsentAgent`

Resource version: `1.0`

create

Usage:

```
am> create OAuth2RemoteConsentAgentGroups --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "remoteConsentResponseEncryptionMethod" : {
      "title" : "Consent response encryption method",
      "description" : "The encryption method to be used by the provider when decrypting the remote
 consent response JWT received from the Remote Consent Service.<br><br>AM supports the following token
```

```
 encryption algorithms: <ul><li><code>A128GCM</code>, <code>A192GCM</code>, and <code>A256GCM</code> -
 AES in Galois Counter Mode (GCM) authenticated encryption mode.</li><li><code>A128CBC-HS256</code>,
 <code>A192CBC-HS384</code>, and <code>A256CBC-HS512</code> - AES encryption in CBC mode, with HMAC-
SHA-2 for integrity.</li></ul>",
      "propertyOrder" : 34600,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "remoteConsentRequestSigningAlgorithm" : {
      "title" : "Consent request Signing Algorithm",
      "description" : "Signing algorithm to be used when signing the consent request JWT.",
      "propertyOrder" : 34500,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "jwksUri" : {
      "title" : "Json Web Key URI",
      "description" : "The URI containing the public keys of the Remote Consent Service secret. The
 public keys are in the Json Web Key (jwk) format.",
      "propertyOrder" : 34800,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "remoteConsentRedirectUrl" : {
      "title" : "Redirect URL",
      "description" : "The Remote Consent Service's URL to which the authorization server should
 redirect the user in order to obtain their consent.",
      "propertyOrder" : 34000,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
    },
    "remoteConsentResponseSigningAlg" : {
      "title" : "Consent response signing algorithm",
      "description" : "The signing algorithm to be used by the provider when verifying the signature
 of the consent response JWT received from the Remote Consent Service.",
      "propertyOrder" : 34400,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
    },
    "remoteConsentRequestEncryptionMethod" : {
      "title" : "Consent request Encryption Method",
      "description" : "Encryption method to be used when encrypting the consent request JWT.",
      "propertyOrder" : 34300,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "publicKeyLocation" : {
      "title" : "Public key selector",
      "description" : "",
      "propertyOrder" : 34700,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
```

```
    },
    "requestTimeLimit" : {
      "title" : "Consent Request Time Limit",
      "description" : "The amount of seconds for which the consent request JWT sent to the Remote
Consent Service should be considered valid.",
      "propertyOrder" : 35200,
      "required" : false,
      "type" : "integer",
      "exampleValue" : ""
    },
    "remoteConsentRequestEncryptionAlgorithm" : {
      "title" : "Consent request Encryption Algorithm",
      "description" : "Encryption algorithm to be used when encrypting the consent request JWT.",
      "propertyOrder" : 34200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "remoteConsentResponseEncryptionAlgorithm" : {
      "title" : "Consent response encryption algorithm",
      "description" : "The encryption algorithm to be used by the provider when decrypting the remote
consent response JWT received from the Remote Consent Service.",
      "propertyOrder" : 34500,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
    },
    "jwkStoreCacheMissCacheTime" : {
      "title" : "JWKs URI content cache miss cache time",
      "description" : "To avoid loading the JWKS URI content for every operation, especially when
the kid is not in the jwks content already cached, the JWKS content will be cached for a minimum
period of time. This cache miss cache time defines the minimum amount of time the JWKS URI content is
cached.",
      "propertyOrder" : 35000,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "jwksCacheTimeout" : {
      "title" : "JWKs URI content cache timeout in ms",
      "description" : "To avoid loading the JWKS URI content for every operation, the JWKS content is
cached. This timeout defines the maximum amount of time the JWKS URI content can be cached before
being refreshed.",
      "propertyOrder" : 34900,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "jwkSet" : {
      "title" : "Json Web Key",
      "description" : "Raw JSON Web Key value containing the Remote Consent Service's public keys.",
      "propertyOrder" : 35100,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
    },
    "remoteConsentRequestEncryptionEnabled" : {
      "title" : "Enable consent request Encryption",
      "description" : "Enables encryption of the consent request JWT.",
```

```
      "propertyOrder" : 34100,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    }
  }
}
```

delete

Usage:

```
am> delete OAuth2RemoteConsentAgentGroups --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action OAuth2RemoteConsentAgentGroups --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action OAuth2RemoteConsentAgentGroups --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action OAuth2RemoteConsentAgentGroups --realm Realm --actionName nextdescendents
```

query

Querying the agent groups of a specific type

Usage:

```
am> query OAuth2RemoteConsentAgentGroups --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read OAuth2RemoteConsentAgentGroups --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update OAuth2RemoteConsentAgentGroups --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "remoteConsentResponseEncryptionMethod" : {
      "title" : "Consent response encryption method",
      "description" : "The encryption method to be used by the provider when decrypting the remote
 consent response JWT received from the Remote Consent Service.<br><br>AM supports the following token
 encryption algorithms: <ul><li><code>A128GCM</code>, <code>A192GCM</code>, and <code>A256GCM</code> -
 AES in Galois Counter Mode (GCM) authenticated encryption mode.</li><li><code>A128CBC-HS256</code>,
 <code>A192CBC-HS384</code>, and <code>A256CBC-HS512</code> - AES encryption in CBC mode, with HMAC-
SHA-2 for integrity.</li></ul>",
      "propertyOrder" : 34600,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "remoteConsentRequestSigningAlgorithm" : {
```

```
      "title" : "Consent request Signing Algorithm",
      "description" : "Signing algorithm to be used when signing the consent request JWT.",
      "propertyOrder" : 34500,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "jwksUri" : {
      "title" : "Json Web Key URI",
      "description" : "The URI containing the public keys of the Remote Consent Service secret. The
public keys are in the Json Web Key (jwk) format.",
      "propertyOrder" : 34800,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "remoteConsentRedirectUrl" : {
      "title" : "Redirect URL",
      "description" : "The Remote Consent Service's URL to which the authorization server should
redirect the user in order to obtain their consent.",
      "propertyOrder" : 34000,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
    },
    "remoteConsentResponseSigningAlg" : {
      "title" : "Consent response signing algorithm",
      "description" : "The signing algorithm to be used by the provider when verifying the signature
of the consent response JWT received from the Remote Consent Service.",
      "propertyOrder" : 34400,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
    },
    "remoteConsentRequestEncryptionMethod" : {
      "title" : "Consent request Encryption Method",
      "description" : "Encryption method to be used when encrypting the consent request JWT.",
      "propertyOrder" : 34300,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "publicKeyLocation" : {
      "title" : "Public key selector",
      "description" : "",
      "propertyOrder" : 34700,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "requestTimeLimit" : {
      "title" : "Consent Request Time Limit",
      "description" : "The amount of seconds for which the consent request JWT sent to the Remote
Consent Service should be considered valid.",
      "propertyOrder" : 35200,
      "required" : false,
      "type" : "integer",
      "exampleValue" : ""
    },
```

```
    "remoteConsentRequestEncryptionAlgorithm" : {
      "title" : "Consent request Encryption Algorithm",
      "description" : "Encryption algorithm to be used when encrypting the consent request JWT.",
      "propertyOrder" : 34200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "remoteConsentResponseEncryptionAlgorithm" : {
      "title" : "Consent response encryption algorithm",
      "description" : "The encryption algorithm to be used by the provider when decrypting the remote
 consent response JWT received from the Remote Consent Service.",
      "propertyOrder" : 34500,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
    },
    "jwkStoreCacheMissCacheTime" : {
      "title" : "JWKs URI content cache miss cache time",
      "description" : "To avoid loading the JWKS URI content for every operation, especially when
 the kid is not in the jwks content already cached, the JWKS content will be cached for a minimum
 period of time. This cache miss cache time defines the minimum amount of time the JWKS URI content is
 cached.",
      "propertyOrder" : 35000,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "jwksCacheTimeout" : {
      "title" : "JWKs URI content cache timeout in ms",
      "description" : "To avoid loading the JWKS URI content for every operation, the JWKS content is
 cached. This timeout defines the maximum amount of time the JWKS URI content can be cached before
 being refreshed.",
      "propertyOrder" : 34900,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "jwkSet" : {
      "title" : "Json Web Key",
      "description" : "Raw JSON Web Key value containing the Remote Consent Service's public keys.",
      "propertyOrder" : 35100,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
    },
    "remoteConsentRequestEncryptionEnabled" : {
      "title" : "Enable consent request Encryption",
      "description" : "Enables encryption of the consent request JWT.",
      "propertyOrder" : 34100,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    }
  }
}
```

OAuth2SoftwarePublisherAgentGroups

Realm Operations

Agent Groups handler that is responsible for managing agent groups

Resource path: `/realm-config/agents/groups/SoftwarePublisher`

Resource version: `1.0`

create

Usage:

```
am> create OAuth2SoftwarePublisherAgentGroups --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "jwkSet" : {
      "title" : "Json Web Key",
      "description" : "Raw JSON Web Key value containing the Software Publisher's public keys.",
      "propertyOrder" : 35100,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
    },
    "issuer" : {
      "title" : "Software publisher issuer",
      "description" : "Identifier for the software publisher, generally represented as a URL.",
      "propertyOrder" : 33001,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "publicKeyLocation" : {
      "title" : "Public key selector",
      "description" : "Select how the Software Publisher's public keys should be retrieved by the
 provider when validating software statement signatures.",
      "propertyOrder" : 34700,
      "required" : false,
```

```
      "type" : "string",
      "exampleValue" : ""
    },
    "softwareStatementSigningAlgorithm" : {
      "title" : "Software statement signing Algorithm",
      "description" : "Signing algorithm to be used when verifying software statement signatures.",
      "propertyOrder" : 34500,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
    },
    "jwkStoreCacheMissCacheTime" : {
      "title" : "JWKs URI content cache miss cache time",
      "description" : "To avoid loading the JWKS URI content for every operation, especially when
 the kid is not in the jwks content already cached, the JWKS content will be cached for a minimum
 period of time. This cache miss cache time defines the minimum amount of time the JWKS URI content is
 cached.",
      "propertyOrder" : 35000,
      "required" : false,
      "type" : "integer",
      "exampleValue" : ""
    },
    "jwksUri" : {
      "title" : "Json Web Key URI",
      "description" : "The URI that contains the Software Publisher's public keys in Json Web Key
 format.",
      "propertyOrder" : 34800,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
    },
    "jwksCacheTimeout" : {
      "title" : "JWKs URI content cache timeout in ms",
      "description" : "To avoid loading the JWKS URI content for every operation, the JWKS content is
 cached. This timeout defines the maximum amount of time the JWKS URI content can be cached before
 being refreshed.",
      "propertyOrder" : 34900,
      "required" : false,
      "type" : "integer",
      "exampleValue" : ""
    }
  }
}
```


delete

Usage:

```
am> delete OAuth2SoftwarePublisherAgentGroups --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action OAuth2SoftwarePublisherAgentGroups --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action OAuth2SoftwarePublisherAgentGroups --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action OAuth2SoftwarePublisherAgentGroups --realm Realm --actionName nextdescendents
```

query

Querying the agent groups of a specific type

Usage:

```
am> query OAuth2SoftwarePublisherAgentGroups --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read OAuth2SoftwarePublisherAgentGroups --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update OAuth2SoftwarePublisherAgentGroups --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "jwkSet" : {
      "title" : "Json Web Key",
      "description" : "Raw JSON Web Key value containing the Software Publisher's public keys.",
      "propertyOrder" : 35100,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
    },
    "issuer" : {
      "title" : "Software publisher issuer",
      "description" : "Identifier for the software publisher, generally represented as a URL.",
      "propertyOrder" : 33001,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "publicKeyLocation" : {
      "title" : "Public key selector",
      "description" : "Select how the Software Publisher's public keys should be retrieved by the
 provider when validating software statement signatures.",
      "propertyOrder" : 34700,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
    },
    "softwareStatementSigningAlgorithm" : {
      "title" : "Software statement signing Algorithm",
      "description" : "Signing algorithm to be used when verifying software statement signatures.",
      "propertyOrder" : 34500,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
    },
    "jwkStoreCacheMissCacheTime" : {
      "title" : "JWKs URI content cache miss cache time",
      "description" : "To avoid loading the JWKS URI content for every operation, especially when
 the kid is not in the jwks content already cached, the JWKS content will be cached for a minimum
```

```
 period of time. This cache miss cache time defines the minimum amount of time the JWKS URI content is
 cached.",
      "propertyOrder" : 35000,
      "required" : false,
      "type" : "integer",
      "exampleValue" : ""
    },
    "jwksUri" : {
      "title" : "Json Web Key URI",
      "description" : "The URI that contains the Software Publisher's public keys in Json Web Key
 format.",
      "propertyOrder" : 34800,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
    },
    "jwksCacheTimeout" : {
      "title" : "JWKs URI content cache timeout in ms",
      "description" : "To avoid loading the JWKS URI content for every operation, the JWKS content is
 cached. This timeout defines the maximum amount of time the JWKS URI content can be cached before
 being refreshed.",
      "propertyOrder" : 34900,
      "required" : false,
      "type" : "integer",
      "exampleValue" : ""
    }
  }
}
```

OAuth2TrustedJWTIssuerAgentGroups

Realm Operations

Agent Groups handler that is responsible for managing agent groups

Resource path: `/realm-config/agents/groups/TrustedJwtIssuer`

Resource version: `1.0`

create

Usage:

```
am> create OAuth2TrustedJWTIssuerAgentGroups --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "jwksUri" : {
      "title" : "JWKs URI",
      "description" : "URI to retrieve JWK verification keys from to validate the JWT signature.",
      "propertyOrder" : 20,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
    },
    "consentedScopesClaim" : {
      "title" : "Consented Scopes Claim",
      "description" : "Optional claim within the JWT that lists the scopes that the user has consented
to. The scopes can be represented either as a JSON array of strings, or as a single space-separated
string.",
      "propertyOrder" : 40,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
    },
    "allowedSubjects" : {
      "title" : "Allowed Subjects",
      "description" : "List of subjects which this provider is allowed to provide consent for. If
blank then the provider can provide consent for any user in this realm.",
      "propertyOrder" : 60,
      "required" : false,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "jwksCacheTimeout" : {
      "title" : "JWKs URI content cache timeout in ms",
      "description" : "To avoid loading the JWKS URI content for every operation, the JWKS content is
cached. This timeout defines the maximum amount of time the JWKS URI content can be cached before
being refreshed.",
      "propertyOrder" : 70,
      "required" : false,
      "type" : "integer",
      "exampleValue" : ""
    },
    "jwkSet" : {
      "title" : "JWK Set",
      "description" : "Manually entered JWK Set of verification keys to validate the JWT signature.",
      "propertyOrder" : 30,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
    },
    "issuer" : {
      "title" : "JWT Issuer",
      "description" : "Expected 'iss' claim identifier for this JWT issuer.",
      "propertyOrder" : 10,
```

```
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "jwkStoreCacheMissCacheTime" : {
      "title" : "JWKs URI content cache miss cache time",
      "description" : "To avoid loading the JWKS URI content for every operation, especially when
 the kid is not in the jwks content already cached, the JWKS content will be cached for a minimum
 period of time. This cache miss cache time defines the minimum amount of time the JWKS URI content is
 cached.",
      "propertyOrder" : 80,
      "required" : false,
      "type" : "integer",
      "exampleValue" : ""
    },
    "resourceOwnerIdentityClaim" : {
      "title" : "Resource Owner Identity Claim",
      "description" : "Claim in the JWT that identifies the resource owner account in AM. Defaults to
 \"sub\".",
      "propertyOrder" : 50,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
```

delete

Usage:

```
am> delete OAuth2TrustedJWTIssuerAgentGroups --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action OAuth2TrustedJWTIssuerAgentGroups --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action OAuth2TrustedJWTIssuerAgentGroups --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action OAuth2TrustedJWTIssuerAgentGroups --realm Realm --actionName nextdescendents
```

query

Querying the agent groups of a specific type

Usage:

```
am> query OAuth2TrustedJWTIssuerAgentGroups --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read OAuth2TrustedJWTIssuerAgentGroups --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update OAuth2TrustedJWTIssuerAgentGroups --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "jwksUri" : {
      "title" : "JWKs URI",
      "description" : "URI to retrieve JWK verification keys from to validate the JWT signature.",
      "propertyOrder" : 20,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
    },
    "consentedScopesClaim" : {
      "title" : "Consented Scopes Claim",
      "description" : "Optional claim within the JWT that lists the scopes that the user has consented
to. The scopes can be represented either as a JSON array of strings, or as a single space-separated
string.",
      "propertyOrder" : 40,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
    },
    "allowedSubjects" : {
      "title" : "Allowed Subjects",
      "description" : "List of subjects which this provider is allowed to provide consent for. If
blank then the provider can provide consent for any user in this realm.",
      "propertyOrder" : 60,
      "required" : false,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "jwksCacheTimeout" : {
      "title" : "JWKs URI content cache timeout in ms",
      "description" : "To avoid loading the JWKS URI content for every operation, the JWKS content is
cached. This timeout defines the maximum amount of time the JWKS URI content can be cached before
being refreshed.",
      "propertyOrder" : 70,
      "required" : false,
      "type" : "integer",
      "exampleValue" : ""
    },
    "jwkSet" : {
      "title" : "JWK Set",
      "description" : "Manually entered JWK Set of verification keys to validate the JWT signature.",
      "propertyOrder" : 30,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
    },
    "issuer" : {
      "title" : "JWT Issuer",
      "description" : "Expected 'iss' claim identifier for this JWT issuer.",
      "propertyOrder" : 10,
```

```
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "jwkStoreCacheMissCacheTime" : {
      "title" : "JWKs URI content cache miss cache time",
      "description" : "To avoid loading the JWKS URI content for every operation, especially when
 the kid is not in the jwks content already cached, the JWKS content will be cached for a minimum
 period of time. This cache miss cache time defines the minimum amount of time the JWKS URI content is
 cached.",
      "propertyOrder" : 80,
      "required" : false,
      "type" : "integer",
      "exampleValue" : ""
    },
    "resourceOwnerIdentityClaim" : {
      "title" : "Resource Owner Identity Claim",
      "description" : "Claim in the JWT that identifies the resource owner account in AM. Defaults to
 \"sub\".",
      "propertyOrder" : 50,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
```

OAuth2UserApplications

Realm Operations

This endpoint exposes a list of all the applications (clients) that the user authorized using OAuth 2.0. Access for those applications can then be revoked on a per-client basis.

Resource path: `/users/{user}/oauth2/applications`

Resource version: `1.1`

delete

Delete the tokens for the specified client ID.

Usage:

```
am> delete OAuth2UserApplications --realm Realm --id id --user user
```

Parameters:

`--id`

The unique identifier for the resource.

--user

This endpoint exposes a list of all the applications (clients) that the user authorized using OAuth 2.0. Access for those applications can then be revoked on a per-client basis.

query

Get a list of the applications that have been granted OAuth 2.0 access. Only `_queryFilter=true` is supported.

Usage:

```
am> query OAuth2UserApplications --realm Realm --filter filter --user user
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

--user

This endpoint exposes a list of all the applications (clients) that the user authorized using OAuth 2.0. Access for those applications can then be revoked on a per-client basis.

OIDCClient

Realm Operations

Resource path: `/realm-config/services/SocialIdentityProviders/oidcConfig`

Resource version: `1.0`

create

Usage:

```
am> create OIDCClient --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "wellKnownEndpoint" : {
      "title" : "Well Known Endpoint",
      "description" : "The endpoint for retrieving a list of OAuth/OIDC endpoints.",
      "propertyOrder" : 1200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "uiConfig" : {
      "title" : "UI Config Properties",
      "description" : "Mapping of display properties to be defined and consumed by the UI.",
      "propertyOrder" : 9999,
      "required" : true,
      "patternProperties" : {
        ".*" : {
          "type" : "string"
        }
      },
      "type" : "object",
      "exampleValue" : ""
    },
    "enabled" : {
      "title" : "Enabled",
      "description" : "",
      "propertyOrder" : 1,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "scopeDelimiter" : {
      "title" : "Scope Delimiter",
      "description" : "The delimiter used by an auth server to separate scopes.",
      "propertyOrder" : 800,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "transform" : {
      "title" : "Transform Script",
      "description" : "A script that takes the raw profile object as input and outputs the normalized
 profile object.",
      "propertyOrder" : 10000,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "basicAuth" : {
      "title" : "Use Basic Auth",
      "description" : "When enabled, the client will use basic auth for authenticating with the social
 auth provider. Enabled by default.",
      "propertyOrder" : 1000,
      "required" : true,
```

```
      "type" : "boolean",
      "exampleValue" : ""
    },
    "userInfoEndpoint" : {
      "title" : "User Profile Service URL",
      "description" : "User profile information URL <p> This URL endpoint provides user profile
information and is provided by the OAuth Identity Provider NB This URL should return JSON objects in
response.",
      "propertyOrder" : 600,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "clientId" : {
      "title" : "Client ID",
      "description" : "OAuth client_id parameter<p> For more information on the OAuth client_id
parameter refer to the RFC 6749 (http://tools.ietf.org/html/rfc6749#section-2.3.1), section 2.3.1.",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "pkceMethod" : {
      "title" : "PKCE Method",
      "description" : "The PKCE transformation method to use when making requests to the authorization
endpoint.",
      "propertyOrder" : 1100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "redirectURI" : {
      "title" : "Redirect URL",
      "description" : "",
      "propertyOrder" : 700,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "authenticationIdKey" : {
      "title" : "Auth ID Key",
      "description" : "Field used to identify a user by the social provider.",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "exampleValue" : "sub"
    },
    "authorizationEndpoint" : {
      "title" : "Authentication Endpoint URL",
      "description" : "OAuth authentication endpoint URL <p> This is the URL endpoint for OAuth
authentication provided by the OAuth Identity Provider.",
      "propertyOrder" : 400,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "clientSecret" : {
      "title" : "Client Secret",
```

```
      "description" : "OAuth client_secret parameter <p>For more information on the OAuth client_id
 parameter refer to the RFC 6749 (http://tools.ietf.org/html/rfc6749#section-2.3.1), section 2.3.1.",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "string",
      "format" : "password",
      "exampleValue" : ""
    },
    "tokenEndpoint" : {
      "title" : "Access Token Endpoint URL",
      "description" : "OAuth access token endpoint URL This is the URL endpoint for access token
 retrieval provided by the OAuth Identity Provider.Refer to the RFC 6749 (http://tools.ietf.org/html/
rfc6749#section-3.2), section 3.2.",
      "propertyOrder" : 500,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "scopes" : {
      "title" : "OAuth Scopes",
      "description" : "List of user profile properties<p>According to the OAuth 2.0 Authorization
 Framework that the client application requires. The list depends on the permissions that the resource
 owner grants to the client application. Some authorization servers use non-standard separators for
 scopes.",
      "propertyOrder" : 900,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "minItems" : 1,
      "type" : "array",
      "exampleValue" : ""
    }
  }
}
```

delete

Usage:

```
am> delete OIDCClient --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action OIDCClient --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action OIDCClient --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action OIDCClient --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query OIDCClient --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read OIDCClient --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update OIDCClient --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "wellKnownEndpoint" : {
      "title" : "Well Known Endpoint",
      "description" : "The endpoint for retrieving a list of OAuth/OIDC endpoints.",
      "propertyOrder" : 1200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "uiConfig" : {
      "title" : "UI Config Properties",
      "description" : "Mapping of display properties to be defined and consumed by the UI.",
      "propertyOrder" : 9999,
      "required" : true,
      "patternProperties" : {
        ".*" : {
          "type" : "string"
        }
      },
      "type" : "object",
      "exampleValue" : ""
    },
    "enabled" : {
      "title" : "Enabled",
      "description" : "",
      "propertyOrder" : 1,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "scopeDelimiter" : {
      "title" : "Scope Delimiter",
      "description" : "The delimiter used by an auth server to separate scopes.",
      "propertyOrder" : 800,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "transform" : {
      "title" : "Transform Script",
      "description" : "A script that takes the raw profile object as input and outputs the normalized
 profile object.",
      "propertyOrder" : 10000,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "basicAuth" : {
      "title" : "Use Basic Auth",
```

```
     "description" : "When enabled, the client will use basic auth for authenticating with the social
auth provider. Enabled by default.",
     "propertyOrder" : 1000,
     "required" : true,
     "type" : "boolean",
     "exampleValue" : ""
   },
   "userInfoEndpoint" : {
     "title" : "User Profile Service URL",
     "description" : "User profile information URL <p> This URL endpoint provides user profile
information and is provided by the OAuth Identity Provider NB This URL should return JSON objects in
response.",
     "propertyOrder" : 600,
     "required" : true,
     "type" : "string",
     "exampleValue" : ""
   },
   "clientId" : {
     "title" : "Client ID",
     "description" : "OAuth client_id parameter<p> For more information on the OAuth client_id
parameter refer to the RFC 6749 (http://tools.ietf.org/html/rfc6749#section-2.3.1), section 2.3.1.",
     "propertyOrder" : 200,
     "required" : true,
     "type" : "string",
     "exampleValue" : ""
   },
   "pkceMethod" : {
     "title" : "PKCE Method",
     "description" : "The PKCE transformation method to use when making requests to the authorization
endpoint.",
     "propertyOrder" : 1100,
     "required" : true,
     "type" : "string",
     "exampleValue" : ""
   },
   "redirectURI" : {
     "title" : "Redirect URL",
     "description" : "",
     "propertyOrder" : 700,
     "required" : true,
     "type" : "string",
     "exampleValue" : ""
   },
   "authenticationIdKey" : {
     "title" : "Auth ID Key",
     "description" : "Field used to identify a user by the social provider.",
     "propertyOrder" : 100,
     "required" : true,
     "type" : "string",
     "exampleValue" : "sub"
   },
   "authorizationEndpoint" : {
     "title" : "Authentication Endpoint URL",
     "description" : "OAuth authentication endpoint URL <p> This is the URL endpoint for OAuth
authentication provided by the OAuth Identity Provider.",
     "propertyOrder" : 400,
     "required" : true,
     "type" : "string",
     "exampleValue" : ""
```

```
    },
    "clientSecret" : {
      "title" : "Client Secret",
      "description" : "OAuth client_secret parameter <p>For more information on the OAuth client_id
 parameter refer to the RFC 6749 (http://tools.ietf.org/html/rfc6749#section-2.3.1), section 2.3.1.",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "string",
      "format" : "password",
      "exampleValue" : ""
    },
    "tokenEndpoint" : {
      "title" : "Access Token Endpoint URL",
      "description" : "OAuth access token endpoint URL This is the URL endpoint for access token
 retrieval provided by the OAuth Identity Provider.Refer to the RFC 6749 (http://tools.ietf.org/html/
rfc6749#section-3.2), section 3.2.",
      "propertyOrder" : 500,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "scopes" : {
      "title" : "OAuth Scopes",
      "description" : "List of user profile properties<p>According to the OAuth 2.0 Authorization
 Framework that the client application requires. The list depends on the permissions that the resource
 owner grants to the client application. Some authorization servers use non-standard separators for
 scopes.",
      "propertyOrder" : 900,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "minItems" : 1,
      "type" : "array",
      "exampleValue" : ""
    }
  }
}
```

OTPCollectorDecision

Realm Operations

Resource path: `/realm-config/authentication/authenticationtrees/nodes/OneTimePasswordCollectorDecisionNode`

Resource version: `1.0`

create

Usage:

```
am> create OTPCollectorDecision --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "passwordExpiryTime" : {
      "title" : "One Time Password Validity Length",
      "description" : "This One Time Password will remain valid for this period in minutes.",
      "propertyOrder" : 100,
      "type" : "integer",
      "exampleValue" : ""
    }
  },
  "required" : [ "passwordExpiryTime" ]
}
```

delete

Usage:

```
am> delete OTPCollectorDecision --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action OTPCollectorDecision --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action OTPCollectorDecision --realm Realm --actionName getCreatableTypes
```

listOutcomes

List the available outcomes for the node type.

Usage:

```
am> action OTPCollectorDecision --realm Realm --body body --actionName listOutcomes
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "title" : "Some configuration of the node. This does not need to be complete against the
 configuration schema."
}
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action OTPCollectorDecision --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query OTPCollectorDecision --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read OTPCollectorDecision --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update OTPCollectorDecision --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "passwordExpiryTime" : {
      "title" : "One Time Password Validity Length",
      "description" : "This One Time Password will remain valid for this period in minutes.",
      "propertyOrder" : 100,
      "type" : "integer",
      "exampleValue" : ""
    }
  },
  "required" : [ "passwordExpiryTime" ]
}
```

OTPEmailSender

Realm Operations

Resource path: `/realm-config/authentication/authenticationtrees/nodes/OneTimePasswordSmtpSenderNode`

Resource version: `1.0`

create

Usage:

```
am> create OTPEmailSender --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "fromEmailAddress" : {
      "title" : "Email From Address",
      "description" : "Emails from the OTP Email Sender node will come from this address.",
      "propertyOrder" : 600,
      "type" : "string",
      "exampleValue" : ""
    },
    "smsGatewayImplementationClass" : {
      "title" : "Gateway Implementation Class",
      "description" : "The OTP Email Sender node uses this class to send email
 messages. <br><br>The gateway class must implement the following interface:
 <br><code>com.sun.identity.authentication.modules.hotp.SMSGateway</code>",
      "propertyOrder" : 2200,
      "type" : "string",
      "exampleValue" : ""
    },
    "sslOption" : {
      "title" : "Mail Server Secure Connection",
      "description" : "This setting controls whether the authentication module communicates with the
 mail server using SSL/TLS.",
      "propertyOrder" : 2100,
      "type" : "string",
      "exampleValue" : ""
    },
    "hostPort" : {
      "title" : "Mail Server Host Port",
      "description" : "The port of the mail server. The default port for SMTP is 25, if using SSL the
 default port is 465.",
      "propertyOrder" : 300,
      "type" : "integer",
      "exampleValue" : ""
    },
    "emailAttribute" : {
      "title" : "Email Attribute Name",
      "description" : "This is the attribute name used by the OTP Sender to email the user.",
      "propertyOrder" : 1100,
      "type" : "string",
      "exampleValue" : ""
    },
    "password" : {
      "title" : "Mail Server Authentication Password",
```

```
      "description" : "The password to use when the mail server is using SMTP authentication.",
      "propertyOrder" : 500,
      "type" : "string",
      "format" : "password",
      "exampleValue" : ""
    },
    "username" : {
      "title" : "Mail Server Authentication Username",
      "description" : "The username to use when the mail server is using SMTP authentication.",
      "propertyOrder" : 400,
      "type" : "string",
      "exampleValue" : ""
    },
    "hostName" : {
      "title" : "Mail Server Host Name",
      "description" : "The name of the mail server OpenAM will use to send the messages.",
      "propertyOrder" : 200,
      "type" : "string",
      "exampleValue" : ""
    }
  },
  "required" : [ "password", "fromEmailAddress", "smsGatewayImplementationClass", "username",
 "hostName", "sslOption", "emailAttribute", "hostPort" ]
}
```

delete

Usage:

```
am> delete OTPEmailSender --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action OTPEmailSender --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action OTPEmailSender --realm Realm --actionName getCreatableTypes
```

listOutcomes

List the available outcomes for the node type.

Usage:

```
am> action OTPEmailSender --realm Realm --body body --actionName listOutcomes
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "title" : "Some configuration of the node. This does not need to be complete against the
 configuration schema."
}
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action OTPEmailSender --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query OTPEmailSender --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read OTPEmailSender --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update OTPEmailSender --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "fromEmailAddress" : {
      "title" : "Email From Address",
      "description" : "Emails from the OTP Email Sender node will come from this address.",
      "propertyOrder" : 600,
      "type" : "string",
      "exampleValue" : ""
    },
    "smsGatewayImplementationClass" : {
      "title" : "Gateway Implementation Class",
      "description" : "The OTP Email Sender node uses this class to send email
 messages. <br><br>The gateway class must implement the following interface:
 <br><code>com.sun.identity.authentication.modules.hotp.SMSGateway</code>",
      "propertyOrder" : 2200,
      "type" : "string",
      "exampleValue" : ""
    },
    "sslOption" : {
      "title" : "Mail Server Secure Connection",
      "description" : "This setting controls whether the authentication module communicates with the
 mail server using SSL/TLS.",
      "propertyOrder" : 2100,
      "type" : "string",
      "exampleValue" : ""
    },
    "hostPort" : {
      "title" : "Mail Server Host Port",
      "description" : "The port of the mail server. The default port for SMTP is 25, if using SSL the
 default port is 465.",
      "propertyOrder" : 300,
      "type" : "integer",
      "exampleValue" : ""
```

```
    },
    "emailAttribute" : {
      "title" : "Email Attribute Name",
      "description" : "This is the attribute name used by the OTP Sender to email the user.",
      "propertyOrder" : 1100,
      "type" : "string",
      "exampleValue" : ""
    },
    "password" : {
      "title" : "Mail Server Authentication Password",
      "description" : "The password to use when the mail server is using SMTP authentication.",
      "propertyOrder" : 500,
      "type" : "string",
      "format" : "password",
      "exampleValue" : ""
    },
    "username" : {
      "title" : "Mail Server Authentication Username",
      "description" : "The username to use when the mail server is using SMTP authentication.",
      "propertyOrder" : 400,
      "type" : "string",
      "exampleValue" : ""
    },
    "hostName" : {
      "title" : "Mail Server Host Name",
      "description" : "The name of the mail server OpenAM will use to send the messages.",
      "propertyOrder" : 200,
      "type" : "string",
      "exampleValue" : ""
    }
  },
  "required" : [ "password", "fromEmailAddress", "smsGatewayImplementationClass", "username",
 "hostName", "sslOption", "emailAttribute", "hostPort" ]
}
```

OTPSMSSender

Realm Operations

Resource path: `/realm-config/authentication/authenticationtrees/nodes/OneTimePasswordSmsSenderNode`

Resource version: `1.0`

create

Usage:

```
am> create OTPSMSSender --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "hostPort" : {
      "title" : "Mail Server Host Port",
      "description" : "The port of the mail server. The default port for SMTP is 25, if using SSL the
 default port is 465.",
      "propertyOrder" : 300,
      "type" : "integer",
      "exampleValue" : ""
    },
    "hostName" : {
      "title" : "Mail Server Host Name",
      "description" : "The name of the mail server OpenAM will use to send the messages.",
      "propertyOrder" : 200,
      "type" : "string",
      "exampleValue" : ""
    },
    "sslOption" : {
      "title" : "Mail Server Secure Connection",
      "description" : "This setting controls whether the authentication module communicates with the
 mail server using SSL/TLS.",
      "propertyOrder" : 2100,
      "type" : "string",
      "exampleValue" : ""
    },
    "username" : {
      "title" : "Mail Server Authentication Username",
      "description" : "The username to use when the mail server is using SMTP authentication.",
      "propertyOrder" : 400,
      "type" : "string",
      "exampleValue" : ""
    },
    "password" : {
      "title" : "Mail Server Authentication Password",
      "description" : "The password to use when the mail server is using SMTP authentication.",
      "propertyOrder" : 500,
      "type" : "string",
      "format" : "password",
      "exampleValue" : ""
    },
    "mobileCarrierAttributeName" : {
      "title" : "Mobile Carrier Attribute Name",
      "description" : "This is the attribute name used for a mobile carrier domain for sending SMS
 messages.",
      "propertyOrder" : 1200,
      "type" : "string",
      "exampleValue" : ""
    },
    "fromEmailAddress" : {
      "title" : "Email From Address",
```

```
      "description" : "Emails from the OTP Email Sender node will come from this address.",
      "propertyOrder" : 600,
      "type" : "string",
      "exampleValue" : ""
    },
    "mobilePhoneAttributeName" : {
      "title" : "Mobile Phone Number Attribute Name",
      "description" : "This is the attribute name used for a requested text message.",
      "propertyOrder" : 1100,
      "type" : "string",
      "exampleValue" : ""
    },
    "smsGatewayImplementationClass" : {
      "title" : "Gateway Implementation Class",
      "description" : "The OTP SMS Sender node uses this class to send SMS
 messages. <br><br>The gateway class must implement the following interface:
 <br><code>com.sun.identity.authentication.modules.hotp.SMSGateway</code>",
      "propertyOrder" : 2200,
      "type" : "string",
      "exampleValue" : ""
    }
  },
  "required" : [ "password", "smsGatewayImplementationClass", "sslOption", "hostPort", "username",
 "fromEmailAddress", "mobilePhoneAttributeName", "hostName" ]
}
```

delete

Usage:

```
am> delete OTPSMSSender --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action OTPSMSSender --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action OTPSMSSender --realm Realm --actionName getCreatableTypes
```

listOutcomes

List the available outcomes for the node type.

Usage:

```
am> action OTPSMSSender --realm Realm --body body --actionName listOutcomes
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "title" : "Some configuration of the node. This does not need to be complete against the
 configuration schema."
}
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action OTPSMSSender --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query OTPSMSSender --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read OTPSMSSender --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update OTPSMSSender --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "hostPort" : {
      "title" : "Mail Server Host Port",
      "description" : "The port of the mail server. The default port for SMTP is 25, if using SSL the
 default port is 465.",
      "propertyOrder" : 300,
      "type" : "integer",
      "exampleValue" : ""
    },
    "hostName" : {
      "title" : "Mail Server Host Name",
      "description" : "The name of the mail server OpenAM will use to send the messages.",
      "propertyOrder" : 200,
      "type" : "string",
      "exampleValue" : ""
    },
    "sslOption" : {
      "title" : "Mail Server Secure Connection",
      "description" : "This setting controls whether the authentication module communicates with the
 mail server using SSL/TLS.",
      "propertyOrder" : 2100,
      "type" : "string",
      "exampleValue" : ""
    },
    "username" : {
      "title" : "Mail Server Authentication Username",
      "description" : "The username to use when the mail server is using SMTP authentication.",
      "propertyOrder" : 400,
      "type" : "string",
      "exampleValue" : ""
    },
    "password" : {
      "title" : "Mail Server Authentication Password",
      "description" : "The password to use when the mail server is using SMTP authentication.",
      "propertyOrder" : 500,
      "type" : "string",
      "format" : "password",
      "exampleValue" : ""
    },
```

```
    "mobileCarrierAttributeName" : {
      "title" : "Mobile Carrier Attribute Name",
      "description" : "This is the attribute name used for a mobile carrier domain for sending SMS
 messages.",
      "propertyOrder" : 1200,
      "type" : "string",
      "exampleValue" : ""
    },
    "fromEmailAddress" : {
      "title" : "Email From Address",
      "description" : "Emails from the OTP Email Sender node will come from this address.",
      "propertyOrder" : 600,
      "type" : "string",
      "exampleValue" : ""
    },
    "mobilePhoneAttributeName" : {
      "title" : "Mobile Phone Number Attribute Name",
      "description" : "This is the attribute name used for a requested text message.",
      "propertyOrder" : 1100,
      "type" : "string",
      "exampleValue" : ""
    },
    "smsGatewayImplementationClass" : {
      "title" : "Gateway Implementation Class",
      "description" : "The OTP SMS Sender node uses this class to send SMS
 messages. <br><br>The gateway class must implement the following interface:
 <br><code>com.sun.identity.authentication.modules.hotp.SMSGateway</code>",
      "propertyOrder" : 2200,
      "type" : "string",
      "exampleValue" : ""
    }
  },
  "required" : [ "password", "smsGatewayImplementationClass", "sslOption", "hostPort", "username",
 "fromEmailAddress", "mobilePhoneAttributeName", "hostName" ]
}
```

OathModule

Realm Operations

Resource path: `/realm-config/authentication/modules/oath`

Resource version: `1.0`

create

Usage:

```
am> create OathModule --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "oathAlgorithm" : {
      "title" : "OATH Algorithm to Use",
      "description" : "Choose the algorithm your device uses to generate the OTP.<br><br>HOTP uses a
counter value that is incremented every time a new OTP is generated. TOTP generates a new OTP every
few seconds as specified by the time step interval.",
      "propertyOrder" : 500,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "truncationOffset" : {
      "title" : "Truncation Offset",
      "description" : "This adds an offset to the generation of the OTP.<br><br>This is an option used
by the HOTP algorithm that not all devices support. This should be left default unless you know your
device uses a offset.",
      "propertyOrder" : 900,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "forgerock-oath-sharedsecret-implementation-class" : {
      "title" : "The Shared Secret Provider Class",
      "description" : "The fully qualified class name for the Shared Secret Provider
extension.<br><br>The class that is used to process the user profile attribute used to store the user
secret key.",
      "propertyOrder" : 1300,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "authenticationLevel" : {
      "title" : "Authentication Level",
      "description" : "The authentication level associated with this module.<br><br>Each
authentication module has an authentication level that can be used to indicate the level of security
associated with the module; 0 is the lowest (and the default).",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "minimumSecretKeyLength" : {
      "title" : "Minimum Secret Key Length",
      "description" : "Number of hexadecimal characters allowed for the Secret Key.",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
```

```
   "timeStepSize" : {
     "title" : "TOTP Time Step Interval",
     "description" : "The TOTP time step in seconds that the OTP device uses to generate the
OTP.<br><br>This is the time interval that one OTP is valid for. For example, if the time step is 30
seconds, then a new OTP will be generated every 30 seconds. This makes a single OTP valid for only 30
seconds.",
     "propertyOrder" : 1000,
     "required" : true,
     "type" : "integer",
     "exampleValue" : ""
   },
   "stepsInWindow" : {
     "title" : "TOTP Time Steps",
     "description" : "The number of time steps to check before and after receiving a OTP.<br><br>This
is the number of time step intervals to check the received OTP against both forward in time and back
in time. For example, with 2 time steps and a time step interval of 30 seconds the server will allow
a clock drift between client and server of 89 seconds. (2-30 second steps and 29 seconds for the
interval that the OTP arrived in)",
     "propertyOrder" : 1100,
     "required" : true,
     "type" : "integer",
     "exampleValue" : ""
   },
   "addChecksum" : {
     "title" : "Add Checksum Digit",
     "description" : "This adds a checksum digit to the OTP.<br><br>This adds a digit to the end
of the OTP generated to be used as a checksum to verify the OTP was generated correctly. This is in
addition to the actual password length. You should only set this if your device supports it.",
     "propertyOrder" : 800,
     "required" : true,
     "type" : "string",
     "exampleValue" : ""
   },
   "secretKeyAttribute" : {
     "title" : "Secret Key Attribute Name",
     "description" : "The name of the attribute in the user profile to store the user secret key.",
     "propertyOrder" : 400,
     "required" : true,
     "type" : "string",
     "exampleValue" : ""
   },
   "lastLoginTimeAttribute" : {
     "title" : "Last Login Time Attribute",
     "description" : "Attribute to store the time of the users last login. This is required if TOTP
is chosen as the OATH algorithm.<br><br>This attribute stores the last time a user logged in to
prevent time based attacks. The value is stored as a number (Unix Time).",
     "propertyOrder" : 1200,
     "required" : true,
     "type" : "string",
     "exampleValue" : ""
   },
   "oathOtpMaxRetry" : {
     "title" : "One Time Password Max Retry",
     "description" : "The number of times entry of the OTP may be attempted. Minimum is 1 maximum is
10 and default is 3.",
     "propertyOrder" : null,
     "required" : true,
     "type" : "integer",
     "exampleValue" : ""
```

```
    },
    "passwordLength" : {
      "title" : "One Time Password Length ",
      "description" : "The length of the generated OTP in digits. Must be 6 digits or longer.",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "forgerock-oath-maximum-clock-drift" : {
      "title" : "Maximum Allowed Clock Drift",
      "description" : "Number of time steps a client is allowed to get out of sync with the server
 before manual resynchronisation is required. This should be greater than the TOTP Time Steps
 value.<br><br>As this checks the time drift over multiple requests it needs to be greater than the
 value specified in TOTP Time Steps.",
      "propertyOrder" : 1500,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "hotpWindowSize" : {
      "title" : "HOTP Window Size",
      "description" : "The size of the window to resynchronize with the client.<br><br>This sets the
 window that the OTP device and the server counter can be out of sync. For example, if the window size
 is 100 and the servers last successful login was at counter value 2, then the server will accept a
 OTP from the OTP device that is from device counter 3 to 102.",
      "propertyOrder" : 600,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "forgerock-oath-observed-clock-drift-attribute-name" : {
      "title" : "Clock Drift Attribute Name",
      "description" : "The name of the attribute in the user profile to store the clock drift. If left
 empty then clock drift checking is disabled.<br><br>The name of the attribute used to store the last
 observed clock drift which is used to indicated when a manual resynchronisation is required.",
      "propertyOrder" : 1400,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "hotpCounterAttribute" : {
      "title" : "Counter Attribute Name",
      "description" : "The name of the attribute in the user profile to store the user counter. This
 is required if HOTP is chosen as the OATH algorithm.",
      "propertyOrder" : 700,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
```

delete

Usage:

```
am> delete OathModule --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action OathModule --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action OathModule --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action OathModule --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query OathModule --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read OathModule --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update OathModule --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "oathAlgorithm" : {
      "title" : "OATH Algorithm to Use",
      "description" : "Choose the algorithm your device uses to generate the OTP.<br><br>HOTP uses a
 counter value that is incremented every time a new OTP is generated. TOTP generates a new OTP every
 few seconds as specified by the time step interval.",
      "propertyOrder" : 500,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "truncationOffset" : {
      "title" : "Truncation Offset",
      "description" : "This adds an offset to the generation of the OTP.<br><br>This is an option used
 by the HOTP algorithm that not all devices support. This should be left default unless you know your
 device uses a offset.",
      "propertyOrder" : 900,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "forgerock-oath-sharedsecret-implementation-class" : {
      "title" : "The Shared Secret Provider Class",
      "description" : "The fully qualified class name for the Shared Secret Provider
 extension.<br><br>The class that is used to process the user profile attribute used to store the user
 secret key.",
      "propertyOrder" : 1300,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
```

```
   },
   "authenticationLevel" : {
     "title" : "Authentication Level",
     "description" : "The authentication level associated with this module.<br><br>Each
authentication module has an authentication level that can be used to indicate the level of security
associated with the module; 0 is the lowest (and the default).",
     "propertyOrder" : 100,
     "required" : true,
     "type" : "integer",
     "exampleValue" : ""
   },
   "minimumSecretKeyLength" : {
     "title" : "Minimum Secret Key Length",
     "description" : "Number of hexadecimal characters allowed for the Secret Key.",
     "propertyOrder" : 300,
     "required" : true,
     "type" : "string",
     "exampleValue" : ""
   },
   "timeStepSize" : {
     "title" : "TOTP Time Step Interval",
     "description" : "The TOTP time step in seconds that the OTP device uses to generate the
OTP.<br><br>This is the time interval that one OTP is valid for. For example, if the time step is 30
seconds, then a new OTP will be generated every 30 seconds. This makes a single OTP valid for only 30
seconds.",
     "propertyOrder" : 1000,
     "required" : true,
     "type" : "integer",
     "exampleValue" : ""
   },
   "stepsInWindow" : {
     "title" : "TOTP Time Steps",
     "description" : "The number of time steps to check before and after receiving a OTP.<br><br>This
is the number of time step intervals to check the received OTP against both forward in time and back
in time. For example, with 2 time steps and a time step interval of 30 seconds the server will allow
a clock drift between client and server of 89 seconds. (2-30 second steps and 29 seconds for the
interval that the OTP arrived in)",
     "propertyOrder" : 1100,
     "required" : true,
     "type" : "integer",
     "exampleValue" : ""
   },
   "addChecksum" : {
     "title" : "Add Checksum Digit",
     "description" : "This adds a checksum digit to the OTP.<br><br>This adds a digit to the end
of the OTP generated to be used as a checksum to verify the OTP was generated correctly. This is in
addition to the actual password length. You should only set this if your device supports it.",
     "propertyOrder" : 800,
     "required" : true,
     "type" : "string",
     "exampleValue" : ""
   },
   "secretKeyAttribute" : {
     "title" : "Secret Key Attribute Name",
     "description" : "The name of the attribute in the user profile to store the user secret key.",
     "propertyOrder" : 400,
     "required" : true,
     "type" : "string",
     "exampleValue" : ""
```

```
   },
   "lastLoginTimeAttribute" : {
     "title" : "Last Login Time Attribute",
     "description" : "Attribute to store the time of the users last login. This is required if TOTP
is chosen as the OATH algorithm.<br><br>This attribute stores the last time a user logged in to
prevent time based attacks. The value is stored as a number (Unix Time).",
     "propertyOrder" : 1200,
     "required" : true,
     "type" : "string",
     "exampleValue" : ""
   },
   "oathOtpMaxRetry" : {
     "title" : "One Time Password Max Retry",
     "description" : "The number of times entry of the OTP may be attempted. Minimum is 1 maximum is
10 and default is 3.",
     "propertyOrder" : null,
     "required" : true,
     "type" : "integer",
     "exampleValue" : ""
   },
   "passwordLength" : {
     "title" : "One Time Password Length ",
     "description" : "The length of the generated OTP in digits. Must be 6 digits or longer.",
     "propertyOrder" : 200,
     "required" : true,
     "type" : "string",
     "exampleValue" : ""
   },
   "forgerock-oath-maximum-clock-drift" : {
     "title" : "Maximum Allowed Clock Drift",
     "description" : "Number of time steps a client is allowed to get out of sync with the server
before manual resynchronisation is required. This should be greater than the TOTP Time Steps
value.<br><br>As this checks the time drift over multiple requests it needs to be greater than the
value specified in TOTP Time Steps.",
     "propertyOrder" : 1500,
     "required" : true,
     "type" : "integer",
     "exampleValue" : ""
   },
   "hotpWindowSize" : {
     "title" : "HOTP Window Size",
     "description" : "The size of the window to resynchronize with the client.<br><br>This sets the
window that the OTP device and the server counter can be out of sync. For example, if the window size
is 100 and the servers last successful login was at counter value 2, then the server will accept a
OTP from the OTP device that is from device counter 3 to 102.",
     "propertyOrder" : 600,
     "required" : true,
     "type" : "integer",
     "exampleValue" : ""
   },
   "forgerock-oath-observed-clock-drift-attribute-name" : {
     "title" : "Clock Drift Attribute Name",
     "description" : "The name of the attribute in the user profile to store the clock drift. If left
empty then clock drift checking is disabled.<br><br>The name of the attribute used to store the last
observed clock drift which is used to indicated when a manual resynchronisation is required.",
     "propertyOrder" : 1400,
     "required" : true,
     "type" : "string",
     "exampleValue" : ""
```

```
    },
    "hotpCounterAttribute" : {
      "title" : "Counter Attribute Name",
      "description" : "The name of the attribute in the user profile to store the user counter. This
 is required if HOTP is chosen as the OATH algorithm.",
      "propertyOrder" : 700,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
```

Global Operations

Resource path: `/global-config/authentication/modules/oath`

Resource version: `1.0`

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action OathModule --global --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action OathModule --global --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action OathModule --global --actionName nextdescendents
```

read

Usage:

```
am> read OathModule --global
```

update

Usage:

```
am> update OathModule --global --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "defaults" : {
      "properties" : {
        "stepsInWindow" : {
          "title" : "TOTP Time Steps",
          "description" : "The number of time steps to check before and after receiving a
OTP.<br><br>This is the number of time step intervals to check the received OTP against both forward
in time and back in time. For example, with 2 time steps and a time step interval of 30 seconds the
server will allow a clock drift between client and server of 89 seconds. (2-30 second steps and 29
seconds for the interval that the OTP arrived in)",
          "propertyOrder" : 1100,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "hotpCounterAttribute" : {
          "title" : "Counter Attribute Name",
          "description" : "The name of the attribute in the user profile to store the user counter.
This is required if HOTP is chosen as the OATH algorithm.",
          "propertyOrder" : 700,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "oathAlgorithm" : {
          "title" : "OATH Algorithm to Use",
          "description" : "Choose the algorithm your device uses to generate the OTP.<br><br>HOTP uses
a counter value that is incremented every time a new OTP is generated. TOTP generates a new OTP every
few seconds as specified by the time step interval.",
          "propertyOrder" : 500,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "timeStepSize" : {
          "title" : "TOTP Time Step Interval",
          "description" : "The TOTP time step in seconds that the OTP device uses to generate the
OTP.<br><br>This is the time interval that one OTP is valid for. For example, if the time step is 30
seconds, then a new OTP will be generated every 30 seconds. This makes a single OTP valid for only 30
seconds.",
          "propertyOrder" : 1000,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
```

```
      },
      "secretKeyAttribute" : {
        "title" : "Secret Key Attribute Name",
        "description" : "The name of the attribute in the user profile to store the user secret
key.",
        "propertyOrder" : 400,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
      },
      "minimumSecretKeyLength" : {
        "title" : "Minimum Secret Key Length",
        "description" : "Number of hexadecimal characters allowed for the Secret Key.",
        "propertyOrder" : 300,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
      },
      "lastLoginTimeAttribute" : {
        "title" : "Last Login Time Attribute",
        "description" : "Attribute to store the time of the users last login. This is required if
TOTP is chosen as the OATH algorithm.<br><br>This attribute stores the last time a user logged in to
prevent time based attacks. The value is stored as a number (Unix Time).",
        "propertyOrder" : 1200,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
      },
      "truncationOffset" : {
        "title" : "Truncation Offset",
        "description" : "This adds an offset to the generation of the OTP.<br><br>This is an option
used by the HOTP algorithm that not all devices support. This should be left default unless you know
your device uses a offset.",
        "propertyOrder" : 900,
        "required" : true,
        "type" : "integer",
        "exampleValue" : ""
      },
      "addChecksum" : {
        "title" : "Add Checksum Digit",
        "description" : "This adds a checksum digit to the OTP.<br><br>This adds a digit to the end
of the OTP generated to be used as a checksum to verify the OTP was generated correctly. This is in
addition to the actual password length. You should only set this if your device supports it.",
        "propertyOrder" : 800,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
      },
      "forgerock-oath-sharedsecret-implementation-class" : {
        "title" : "The Shared Secret Provider Class",
        "description" : "The fully qualified class name for the Shared Secret Provider
extension.<br><br>The class that is used to process the user profile attribute used to store the user
secret key.",
        "propertyOrder" : 1300,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
      },
      "authenticationLevel" : {
```

```
          "title" : "Authentication Level",
          "description" : "The authentication level associated with this module.<br><br>Each
authentication module has an authentication level that can be used to indicate the level of security
associated with the module; 0 is the lowest (and the default).",
          "propertyOrder" : 100,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "forgerock-oath-maximum-clock-drift" : {
          "title" : "Maximum Allowed Clock Drift",
          "description" : "Number of time steps a client is allowed to get out of sync with the
server before manual resynchronisation is required. This should be greater than the TOTP Time Steps
value.<br><br>As this checks the time drift over multiple requests it needs to be greater than the
value specified in TOTP Time Steps.",
          "propertyOrder" : 1500,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "oathOtpMaxRetry" : {
          "title" : "One Time Password Max Retry",
          "description" : "The number of times entry of the OTP may be attempted. Minimum is 1 maximum
is 10 and default is 3.",
          "propertyOrder" : null,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "hotpWindowSize" : {
          "title" : "HOTP Window Size",
          "description" : "The size of the window to resynchronize with the client.<br><br>This sets
the window that the OTP device and the server counter can be out of sync. For example, if the window
size is 100 and the servers last successful login was at counter value 2, then the server will accept
a OTP from the OTP device that is from device counter 3 to 102.",
          "propertyOrder" : 600,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "forgerock-oath-observed-clock-drift-attribute-name" : {
          "title" : "Clock Drift Attribute Name",
          "description" : "The name of the attribute in the user profile to store the clock drift. If
left empty then clock drift checking is disabled.<br><br>The name of the attribute used to store the
last observed clock drift which is used to indicated when a manual resynchronisation is required.",
          "propertyOrder" : 1400,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "passwordLength" : {
          "title" : "One Time Password Length ",
          "description" : "The length of the generated OTP in digits. Must be 6 digits or longer.",
          "propertyOrder" : 200,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      },
```

```
      "type" : "object",
      "title" : "Realm Defaults"
    }
  }
}
```

OathUserDevices

Realm Operations

The Oath devices service is responsible for exposing functions to change the collection of OATH authentication devices. The supported methods are action, delete, query

Resource path: `/users/{user}/devices/2fa/oath`

Resource version: `1.0`

check

Checks if the user's Authenticator OATH module is 'skippable' and returns the result as a boolean

Usage:

```
am> action OathUserDevices --realm Realm --body body --user user --actionName check
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "$schema" : "http://json-schema.org/draft-04/schema#",
  "description" : "OATH user device check action request schema",
  "type" : "object",
  "title" : "OATH user device check action request schema"
}
```

--user

The Oath devices service is responsible for exposing functions to change the collection of OATH authentication devices. The supported methods are action, delete, query

delete

Delete OATH user device

Usage:

```
am> delete OathUserDevices --realm Realm --id id --user user
```

Parameters:

--id

The unique identifier for the resource.

--user

The Oath devices service is responsible for exposing functions to change the collection of OATH authentication devices. The supported methods are action, delete, query

query

Query the user's device profile

Usage:

```
am> query OathUserDevices --realm Realm --filter filter --user user
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all. Fields that can be queried: [*]

--user

The Oath devices service is responsible for exposing functions to change the collection of OATH authentication devices. The supported methods are action, delete, query

reset

Sets the user's 'skippable' selection of Authenticator OATH module to default (NOT_SET) and deletes their profiles attribute

Usage:

```
am> action OathUserDevices --realm Realm --body body --user user --actionName reset
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "description" : "OATH user device reset action request schema",
  "type" : "object",
  "title" : "OATH user device reset action request schema"
}
```

--user

The Oath devices service is responsible for exposing functions to change the collection of OATH authentication devices. The supported methods are action, delete, query

skip

Sets the user's ability to skip an Authenticator OATH module

Usage:

```
am> action OathUserDevices --realm Realm --body body --user user --actionName skip
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "description" : "OATH user device skip action request schema",
  "type" : "object",
  "title" : "OATH user device skip action request schema",
  "properties" : {
    "value" : {
      "type" : "boolean",
      "title" : "Skip OATH module response value",
      "description" : "True if the OATH device is set to skipped"
    }
  },
  "required" : [ "value" ]
}
```

--user

The Oath devices service is responsible for exposing functions to change the collection of OATH authentication devices. The supported methods are action, delete, query

OpenDJ

Realm Operations

Resource path: `/realm-config/services/id-repositories/LDAPv3ForOpenDS`

Resource version: `1.0`

create

Usage:

```
am> create OpenDJ --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "groupconfig" : {
      "type" : "object",
      "title" : "Group Configuration",
      "propertyOrder" : 5,
      "properties" : {
        "sun-idrepo-ldapv3-config-memberof" : {
          "title" : "Attribute Name for Group Membership",
          "description" : "",
          "propertyOrder" : 3500,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-groups-search-filter" : {
          "title" : "LDAP Groups Search Filter",
          "description" : "",
          "propertyOrder" : 3000,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-uniquemember" : {
          "title" : "Attribute Name of Unique Member",
          "description" : "",
          "propertyOrder" : 3600,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-group-attributes" : {
          "title" : "LDAP Groups Attributes",
          "description" : "",
          "propertyOrder" : 3400,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-groups-search-attribute" : {
          "title" : "LDAP Groups Search Attribute",
          "description" : "",
```

```
          "propertyOrder" : 2900,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-group-objectclass" : {
          "title" : "LDAP Groups Object Class",
          "description" : "",
          "propertyOrder" : 3300,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-memberurl" : {
          "title" : "Attribute Name of Group Member URL",
          "description" : "",
          "propertyOrder" : 3700,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-group-container-value" : {
          "title" : "LDAP Groups Container Value",
          "description" : "",
          "propertyOrder" : 3200,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-group-container-name" : {
          "title" : "LDAP Groups Container Naming Attribute",
          "description" : "",
          "propertyOrder" : 3100,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "userconfig" : {
      "type" : "object",
      "title" : "User Configuration",
      "propertyOrder" : 3,
      "properties" : {
        "sun-idrepo-ldapv3-config-people-container-name" : {
          "title" : "LDAP People Container Naming Attribute",
          "description" : "",
          "propertyOrder" : 5000,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-users-search-attribute" : {
          "title" : "LDAP Users  Search Attribute",
          "description" : "",
          "propertyOrder" : 2100,
```

```
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-user-attributes" : {
          "title" : "LDAP User Attributes",
          "description" : "",
          "propertyOrder" : 2400,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-auth-kba-index-attr" : {
          "title" : "Knowledge Based Authentication Active Index",
          "description" : "",
          "propertyOrder" : 5400,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-auth-kba-attempts-attr" : {
          "title" : "Knowledge Based Authentication Attempts Attribute Name",
          "description" : "",
          "propertyOrder" : 5410,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-createuser-attr-mapping" : {
          "title" : "Create User Attribute Mapping",
          "description" : "Format: attribute name or TargetAttributeName=SourceAttributeName",
          "propertyOrder" : 2500,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-people-container-value" : {
          "title" : "LDAP People Container Value",
          "description" : "",
          "propertyOrder" : 5100,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-users-search-filter" : {
          "title" : "LDAP Users  Search Filter",
          "description" : "",
          "propertyOrder" : 2200,
          "required" : false,
          "type" : "string",
```

```
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-user-objectclass" : {
          "title" : "LDAP User Object Class",
          "description" : "",
          "propertyOrder" : 2300,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-inactive" : {
          "title" : "User Status Inactive Value",
          "description" : "",
          "propertyOrder" : 2800,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-auth-kba-attr" : {
          "title" : "Knowledge Based Authentication Attribute Name",
          "description" : "",
          "propertyOrder" : 5300,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-isactive" : {
          "title" : "Attribute Name of User Status",
          "description" : "",
          "propertyOrder" : 2600,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-active" : {
          "title" : "User Status Active Value",
          "description" : "",
          "propertyOrder" : 2700,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "ldapsettings" : {
      "type" : "object",
      "title" : "Server Settings",
      "propertyOrder" : 0,
      "properties" : {
        "sun-idrepo-ldapv3-config-max-result" : {
          "title" : "Maximum Results Returned from Search",
          "description" : "",
          "propertyOrder" : 1500,
```

```
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "openam-idrepo-ldapv3-affinity-enabled" : {
          "title" : "Affinity Enabled",
          "description" : "Enables affinity based request load balancing when accessing the user store
servers (based on DN). It is imperative that the connection string setting is set to the same value
for all OpenAM servers in the deployment when this feature is enabled.",
          "propertyOrder" : 6300,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "openam-idrepo-ldapv3-proxied-auth-denied-fallback" : {
          "title" : "Fallback using Bind DN if Proxied Authorization denied",
          "description" : "Enable this setting to fallback and retry using non-proxied authorization
(DS proxied-auth privilege) when proxied authorization is denied. Normally this happens when the
attributes cannot be changed because the account is locked or the password has expired. This setting
is effective only when Proxied Authorization is enabled.",
          "propertyOrder" : 860,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "openam-idrepo-ldapv3-heartbeat-timeunit" : {
          "title" : "LDAP Connection Heartbeat Time Unit",
          "description" : "Defines the time unit corresponding to the Heartbeat Interval
setting.<br><br>This setting controls how often OpenAM <b>should</b> send a heartbeat search request
to the configured directory. If a connection becomes unresponsive (e.g. due to a network error) then
it may take up to the interval period before the problem is detected. Use along with the Heartbeat
Interval parameter to define the exact interval.",
          "propertyOrder" : 1400,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-search-scope" : {
          "title" : "LDAPv3 Plug-in Search Scope",
          "description" : "",
          "propertyOrder" : 2000,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-authpw" : {
          "title" : "LDAP Bind Password",
          "description" : "",
          "propertyOrder" : 800,
          "required" : false,
          "type" : "string",
          "format" : "password",
          "exampleValue" : ""
        },
        "openam-idrepo-ldapv3-heartbeat-interval" : {
          "title" : "LDAP Connection Heartbeat Interval",
          "description" : "Specifies how often should OpenAM send a heartbeat request to the
directory.<br><br>This setting controls how often OpenAM <b>should</b> send a heartbeat search
request to the configured directory. If a connection becomes unresponsive (e.g. due to a network
```

```
error) then it may take up to the interval period before the problem is detected. Use along with the
Heartbeat Time Unit parameter to define the exact interval. Zero or negative value will result in
disabling heartbeat requests.",
          "propertyOrder" : 1300,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-authid" : {
          "title" : "LDAP Bind DN",
          "description" : "A user or admin with sufficient access rights to perform the supported
operations.",
          "propertyOrder" : 700,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-ldap-server" : {
          "title" : "LDAP Server",
          "description" : "Format: LDAP server host name:port | server_ID | site_ID",
          "propertyOrder" : 600,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "minItems" : 1,
          "type" : "array",
          "exampleValue" : ""
        },
        "openam-idrepo-ldapv3-proxied-auth-enabled" : {
          "title" : "Proxied Authorization using Bind DN",
          "description" : "Enable this setting if you have configured the LDAP bind DN account for
proxied authorization (DS proxied-auth privilege). Do not enable this property if the LDAP bind DN
account does not have the proxied-auth privilege granted because the user would not be able to reset
their password. DS and AM log an error when this occurs.",
          "propertyOrder" : 850,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-connection_pool_max_size" : {
          "title" : "LDAP Connection Pool Maximum Size",
          "description" : "",
          "propertyOrder" : 1200,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-connection_pool_min_size" : {
          "title" : "LDAP Connection Pool Minimum Size",
          "description" : "",
          "propertyOrder" : 1100,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "openam-idrepo-ldapv3-behera-support-enabled" : {
          "title" : "Behera Support Enabled",
```

```
          "description" : "When enabled, Behera draft control will be used in the outgoing requests
for operations that may modify password value. This will allow OpenAM to display password policy
related error messages when password policies are not met.",
          "propertyOrder" : 6100,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-organization_name" : {
          "title" : "LDAP Organization DN",
          "description" : "",
          "propertyOrder" : 900,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-connection-mode" : {
          "title" : "LDAP Connection Mode",
          "description" : "Defines which protocol/operation is used to establish the connection to
the LDAP Directory Server.<br><br>If 'LDAP' is selected, the connection <b>won't be secured</b> and
passwords are transferred in <b>cleartext</b> over the network.<br/> If 'LDAPS' is selected, the
connection is secured via SSL or TLS. <br/> If 'StartTLS' is selected, the connection is secured by
using StartTLS extended operation.",
          "propertyOrder" : 1000,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-time-limit" : {
          "title" : "Search Timeout",
          "description" : "In seconds.",
          "propertyOrder" : 1600,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        }
      }
    },
    "pluginconfig" : {
      "type" : "object",
      "title" : "Plug-in Configuration",
      "propertyOrder" : 2,
      "properties" : {
        "sunIdRepoClass" : {
          "title" : "LDAPv3 Repository Plug-in Class Name",
          "description" : "",
          "propertyOrder" : 1700,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "sunIdRepoAttributeMapping" : {
          "title" : "Attribute Name Mapping",
          "description" : "",
          "propertyOrder" : 1800,
          "required" : false,
          "items" : {
            "type" : "string"
          },
```

```
          "type" : "array",
          "exampleValue" : ""
        },
        "sunIdRepoSupportedOperations" : {
          "title" : "LDAPv3 Plug-in Supported Types and Operations",
          "description" : "",
          "propertyOrder" : 1900,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        }
      }
    },
    "cachecontrol" : {
      "type" : "object",
      "title" : "Cache Control",
      "propertyOrder" : 9,
      "properties" : {
        "sun-idrepo-ldapv3-dncache-size" : {
          "title" : "DN Cache Size",
          "description" : "In DN items, only used when DN Cache is enabled.",
          "propertyOrder" : 6000,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-dncache-enabled" : {
          "title" : "DN Cache",
          "description" : "Used to enable/disable the DN Cache within the OpenAM repository
implementation.<br><br>The DN Cache is used to cache DN lookups which tend to happen in bursts during
authentication. The DN Cache can become out of date when a user is moved or renamed in the underlying
LDAP store and this is not reflected in a persistent search result. Enable when the underlying LDAP
store supports persistent search and move/rename (mod_dn) results are available.",
          "propertyOrder" : 5900,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        }
      }
    },
    "persistentsearch" : {
      "type" : "object",
      "title" : "Persistent Search Controls",
      "propertyOrder" : 7,
      "properties" : {
        "sun-idrepo-ldapv3-config-psearchbase" : {
          "title" : "Persistent Search Base DN",
          "description" : "",
          "propertyOrder" : 5500,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-psearch-scope" : {
          "title" : "Persistent Search Scope",
          "description" : "",
```

```
          "propertyOrder" : 5700,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-psearch-filter" : {
          "title" : "Persistent Search Filter",
          "description" : "",
          "propertyOrder" : 5600,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "errorhandling" : {
      "type" : "object",
      "title" : "Error Handling Configuration",
      "propertyOrder" : 8,
      "properties" : {
        "com.iplanet.am.ldap.connection.delay.between.retries" : {
          "title" : "The Delay Time Between Retries",
          "description" : "In milliseconds.",
          "propertyOrder" : 5800,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        }
      }
    },
    "authentication" : {
      "type" : "object",
      "title" : "Authentication Configuration",
      "propertyOrder" : 4,
      "properties" : {
        "sun-idrepo-ldapv3-config-auth-naming-attr" : {
          "title" : "Authentication Naming Attribute",
          "description" : "",
          "propertyOrder" : 5200,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    }
  }
}
```

delete

Usage:

```
am> delete OpenDJ --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action OpenDJ --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action OpenDJ --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action OpenDJ --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query OpenDJ --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read OpenDJ --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update OpenDJ --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "groupconfig" : {
      "type" : "object",
      "title" : "Group Configuration",
      "propertyOrder" : 5,
      "properties" : {
        "sun-idrepo-ldapv3-config-memberof" : {
          "title" : "Attribute Name for Group Membership",
          "description" : "",
          "propertyOrder" : 3500,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-groups-search-filter" : {
          "title" : "LDAP Groups Search Filter",
          "description" : "",
          "propertyOrder" : 3000,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-uniquemember" : {
          "title" : "Attribute Name of Unique Member",
          "description" : "",
          "propertyOrder" : 3600,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-group-attributes" : {
          "title" : "LDAP Groups Attributes",
          "description" : "",
          "propertyOrder" : 3400,
```

```
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-groups-search-attribute" : {
          "title" : "LDAP Groups Search Attribute",
          "description" : "",
          "propertyOrder" : 2900,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-group-objectclass" : {
          "title" : "LDAP Groups Object Class",
          "description" : "",
          "propertyOrder" : 3300,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-memberurl" : {
          "title" : "Attribute Name of Group Member URL",
          "description" : "",
          "propertyOrder" : 3700,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-group-container-value" : {
          "title" : "LDAP Groups Container Value",
          "description" : "",
          "propertyOrder" : 3200,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-group-container-name" : {
          "title" : "LDAP Groups Container Naming Attribute",
          "description" : "",
          "propertyOrder" : 3100,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "userconfig" : {
      "type" : "object",
      "title" : "User Configuration",
      "propertyOrder" : 3,
      "properties" : {
        "sun-idrepo-ldapv3-config-people-container-name" : {
          "title" : "LDAP People Container Naming Attribute",
```

```
          "description" : "",
          "propertyOrder" : 5000,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-users-search-attribute" : {
          "title" : "LDAP Users  Search Attribute",
          "description" : "",
          "propertyOrder" : 2100,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-user-attributes" : {
          "title" : "LDAP User Attributes",
          "description" : "",
          "propertyOrder" : 2400,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-auth-kba-index-attr" : {
          "title" : "Knowledge Based Authentication Active Index",
          "description" : "",
          "propertyOrder" : 5400,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-auth-kba-attempts-attr" : {
          "title" : "Knowledge Based Authentication Attempts Attribute Name",
          "description" : "",
          "propertyOrder" : 5410,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-createuser-attr-mapping" : {
          "title" : "Create User Attribute Mapping",
          "description" : "Format: attribute name or TargetAttributeName=SourceAttributeName",
          "propertyOrder" : 2500,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-people-container-value" : {
          "title" : "LDAP People Container Value",
          "description" : "",
          "propertyOrder" : 5100,
```

```
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-users-search-filter" : {
          "title" : "LDAP Users  Search Filter",
          "description" : "",
          "propertyOrder" : 2200,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-user-objectclass" : {
          "title" : "LDAP User Object Class",
          "description" : "",
          "propertyOrder" : 2300,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-inactive" : {
          "title" : "User Status Inactive Value",
          "description" : "",
          "propertyOrder" : 2800,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-auth-kba-attr" : {
          "title" : "Knowledge Based Authentication Attribute Name",
          "description" : "",
          "propertyOrder" : 5300,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-isactive" : {
          "title" : "Attribute Name of User Status",
          "description" : "",
          "propertyOrder" : 2600,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-active" : {
          "title" : "User Status Active Value",
          "description" : "",
          "propertyOrder" : 2700,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        }
      }
```

```
   },
   "ldapsettings" : {
     "type" : "object",
     "title" : "Server Settings",
     "propertyOrder" : 0,
     "properties" : {
       "sun-idrepo-ldapv3-config-max-result" : {
         "title" : "Maximum Results Returned from Search",
         "description" : "",
         "propertyOrder" : 1500,
         "required" : false,
         "type" : "integer",
         "exampleValue" : ""
       },
       "openam-idrepo-ldapv3-affinity-enabled" : {
         "title" : "Affinity Enabled",
         "description" : "Enables affinity based request load balancing when accessing the user store
servers (based on DN). It is imperative that the connection string setting is set to the same value
for all OpenAM servers in the deployment when this feature is enabled.",
         "propertyOrder" : 6300,
         "required" : true,
         "type" : "boolean",
         "exampleValue" : ""
       },
       "openam-idrepo-ldapv3-proxied-auth-denied-fallback" : {
         "title" : "Fallback using Bind DN if Proxied Authorization denied",
         "description" : "Enable this setting to fallback and retry using non-proxied authorization
(DS proxied-auth privilege) when proxied authorization is denied. Normally this happens when the
attributes cannot be changed because the account is locked or the password has expired. This setting
is effective only when Proxied Authorization is enabled.",
         "propertyOrder" : 860,
         "required" : false,
         "type" : "boolean",
         "exampleValue" : ""
       },
       "openam-idrepo-ldapv3-heartbeat-timeunit" : {
         "title" : "LDAP Connection Heartbeat Time Unit",
         "description" : "Defines the time unit corresponding to the Heartbeat Interval
setting.<br><br>This setting controls how often OpenAM <b>should</b> send a heartbeat search request
to the configured directory. If a connection becomes unresponsive (e.g. due to a network error) then
it may take up to the interval period before the problem is detected. Use along with the Heartbeat
Interval parameter to define the exact interval.",
         "propertyOrder" : 1400,
         "required" : false,
         "type" : "string",
         "exampleValue" : ""
       },
       "sun-idrepo-ldapv3-config-search-scope" : {
         "title" : "LDAPv3 Plug-in Search Scope",
         "description" : "",
         "propertyOrder" : 2000,
         "required" : false,
         "type" : "string",
         "exampleValue" : ""
       },
       "sun-idrepo-ldapv3-config-authpw" : {
         "title" : "LDAP Bind Password",
         "description" : "",
         "propertyOrder" : 800,
```

```
          "required" : false,
          "type" : "string",
          "format" : "password",
          "exampleValue" : ""
        },
        "openam-idrepo-ldapv3-heartbeat-interval" : {
          "title" : "LDAP Connection Heartbeat Interval",
          "description" : "Specifies how often should OpenAM send a heartbeat request to the
directory.<br><br>This setting controls how often OpenAM <b>should</b> send a heartbeat search
request to the configured directory. If a connection becomes unresponsive (e.g. due to a network
error) then it may take up to the interval period before the problem is detected. Use along with the
Heartbeat Time Unit parameter to define the exact interval. Zero or negative value will result in
disabling heartbeat requests.",
          "propertyOrder" : 1300,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-authid" : {
          "title" : "LDAP Bind DN",
          "description" : "A user or admin with sufficient access rights to perform the supported
operations.",
          "propertyOrder" : 700,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-ldap-server" : {
          "title" : "LDAP Server",
          "description" : "Format: LDAP server host name:port | server_ID | site_ID",
          "propertyOrder" : 600,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "minItems" : 1,
          "type" : "array",
          "exampleValue" : ""
        },
        "openam-idrepo-ldapv3-proxied-auth-enabled" : {
          "title" : "Proxied Authorization using Bind DN",
          "description" : "Enable this setting if you have configured the LDAP bind DN account for
proxied authorization (DS proxied-auth privilege). Do not enable this property if the LDAP bind DN
account does not have the proxied-auth privilege granted because the user would not be able to reset
their password. DS and AM log an error when this occurs.",
          "propertyOrder" : 850,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-connection_pool_max_size" : {
          "title" : "LDAP Connection Pool Maximum Size",
          "description" : "",
          "propertyOrder" : 1200,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-connection_pool_min_size" : {
```

```
          "title" : "LDAP Connection Pool Minimum Size",
          "description" : "",
          "propertyOrder" : 1100,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "openam-idrepo-ldapv3-behera-support-enabled" : {
          "title" : "Behera Support Enabled",
          "description" : "When enabled, Behera draft control will be used in the outgoing requests
for operations that may modify password value. This will allow OpenAM to display password policy
related error messages when password policies are not met.",
          "propertyOrder" : 6100,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-organization_name" : {
          "title" : "LDAP Organization DN",
          "description" : "",
          "propertyOrder" : 900,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-connection-mode" : {
          "title" : "LDAP Connection Mode",
          "description" : "Defines which protocol/operation is used to establish the connection to
the LDAP Directory Server.<br><br>If 'LDAP' is selected, the connection <b>won't be secured</b> and
passwords are transferred in <b>cleartext</b> over the network.<br/> If 'LDAPS' is selected, the
connection is secured via SSL or TLS. <br/> If 'StartTLS' is selected, the connection is secured by
using StartTLS extended operation.",
          "propertyOrder" : 1000,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-time-limit" : {
          "title" : "Search Timeout",
          "description" : "In seconds.",
          "propertyOrder" : 1600,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        }
      }
    },
    "pluginconfig" : {
      "type" : "object",
      "title" : "Plug-in Configuration",
      "propertyOrder" : 2,
      "properties" : {
        "sunIdRepoClass" : {
          "title" : "LDAPv3 Repository Plug-in Class Name",
          "description" : "",
          "propertyOrder" : 1700,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
```

```
        },
        "sunIdRepoAttributeMapping" : {
          "title" : "Attribute Name Mapping",
          "description" : "",
          "propertyOrder" : 1800,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "sunIdRepoSupportedOperations" : {
          "title" : "LDAPv3 Plug-in Supported Types and Operations",
          "description" : "",
          "propertyOrder" : 1900,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        }
      }
    },
    "cachecontrol" : {
      "type" : "object",
      "title" : "Cache Control",
      "propertyOrder" : 9,
      "properties" : {
        "sun-idrepo-ldapv3-dncache-size" : {
          "title" : "DN Cache Size",
          "description" : "In DN items, only used when DN Cache is enabled.",
          "propertyOrder" : 6000,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-dncache-enabled" : {
          "title" : "DN Cache",
          "description" : "Used to enable/disable the DN Cache within the OpenAM repository
implementation.<br><br>The DN Cache is used to cache DN lookups which tend to happen in bursts during
authentication. The DN Cache can become out of date when a user is moved or renamed in the underlying
LDAP store and this is not reflected in a persistent search result. Enable when the underlying LDAP
store supports persistent search and move/rename (mod_dn) results are available.",
          "propertyOrder" : 5900,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        }
      }
    },
    "persistentsearch" : {
      "type" : "object",
      "title" : "Persistent Search Controls",
      "propertyOrder" : 7,
      "properties" : {
        "sun-idrepo-ldapv3-config-psearchbase" : {
          "title" : "Persistent Search Base DN",
```

```
          "description" : "",
          "propertyOrder" : 5500,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-psearch-scope" : {
          "title" : "Persistent Search Scope",
          "description" : "",
          "propertyOrder" : 5700,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-psearch-filter" : {
          "title" : "Persistent Search Filter",
          "description" : "",
          "propertyOrder" : 5600,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "errorhandling" : {
      "type" : "object",
      "title" : "Error Handling Configuration",
      "propertyOrder" : 8,
      "properties" : {
        "com.iplanet.am.ldap.connection.delay.between.retries" : {
          "title" : "The Delay Time Between Retries",
          "description" : "In milliseconds.",
          "propertyOrder" : 5800,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        }
      }
    },
    "authentication" : {
      "type" : "object",
      "title" : "Authentication Configuration",
      "propertyOrder" : 4,
      "properties" : {
        "sun-idrepo-ldapv3-config-auth-naming-attr" : {
          "title" : "Authentication Naming Attribute",
          "description" : "",
          "propertyOrder" : 5200,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    }
  }
}
```

OpenIDConnect

Realm Operations

Resource path: `/realm-config/authentication/authenticationtrees/nodes/SocialOpenIdConnectNode`

Resource version: `1.0`

create

Usage:

```
am> create OpenIDConnect --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "cfgMixUpMitigation" : {
      "title" : "OAuth 2.0 Mix-Up Mitigation Enabled",
      "description" : "Enables OAuth 2.0 mix-up mitigation The authorization server must support
 the OAuth 2.0 Mix-Up Mitigation draft (https://tools.ietf.org/html/draft-ietf-oauth-mix-up-
mitigation-01#section-3.1), otherwise OpenAM will fail to validate responses from the authorization
 server. If only the OAuth 2.0 protocol is utilized, make sure that the accepted issuer value is set
 in the \"Token Issuer\" setting.",
      "propertyOrder" : 1700,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "openIdValidationMethod" : {
      "title" : "OpenID Connect Validation Type",
      "description" : "In order to validate the ID token from the OpenID Connect provider, the node
 needs either a URL to get the public keys for the provider, or the symmetric key for an ID token
 signed with a HMAC-based algorithm. <p> By default, the configuration type is .well-known/openid-
configuration_url. This means the node should retrieve the keys based on information in the OpenID
 Connect Provider Configuration Document. <p>You can instead configure the authentication node to
 validate the ID token signature with the client secret key you provide, or to validate the ID token
 with the keys retrieved from the URL to the OpenID Connect provider's JSON web key set.",
      "propertyOrder" : 1900,
      "type" : "string",
      "exampleValue" : ""
    },
    "cfgAttributeMappingConfiguration" : {
      "title" : "Attribute Mapper Configuration",
```

```
      "description" : "Mapping of OAuth attributes to local OpenAM attributes Attribute configuration
 that will be used to map the user info obtained from the OAuth 2.0 Provider to the local user data
 store in the OpenAM. Example: OAuth2.0_attribute=local_attribute",
      "propertyOrder" : 1500,
      "patternProperties" : {
        ".*" : {
          "type" : "string"
        }
      },
      "type" : "object",
      "exampleValue" : ""
    },
    "provider" : {
      "title" : "Social Provider",
      "description" : "Social Provider for which this node is being setup.",
      "propertyOrder" : 800,
      "type" : "string",
      "exampleValue" : ""
    },
    "authenticationIdKey" : {
      "title" : "Auth ID Key",
      "description" : "",
      "propertyOrder" : 900,
      "type" : "string",
      "exampleValue" : ""
    },
    "issuer" : {
      "title" : "Token Issuer",
      "description" : "Required when the 'openid' scope is included. Value must match the iss field in
 issued ID Token e.g. <code>accounts.google.com</code> The issuer value MUST be provided when OAuth
 2.0 Mix-Up Mitigation is enabled.",
      "propertyOrder" : 1800,
      "type" : "string",
      "exampleValue" : ""
    },
    "cfgAccountMapperClass" : {
      "title" : "Account Mapper",
      "description" : "Name of the class implementing the attribute mapping for the
 account search. This class is used by the node to map from the account information
 received from the OAuth Identity Provider into OpenAM. The class must implement the
 <code>org.forgerock.openam.authentication.modules.common.mapping.AttributeMapper</code> interface.
 Provided implementations are:
 <code>org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper
 org.forgerock.openam.authentication.modules.oidc.JwtAttributeMapper</code> (canonly be used when
 using the openid scope) String constructor parameters can be provided by appending | separated
 values.",
      "propertyOrder" : 1200,
      "type" : "string",
      "exampleValue" : ""
    },
    "tokenEndpoint" : {
      "title" : "Access Token Endpoint URL",
      "description" : "OAuth access token endpoint URL This is the URL endpoint for access token
 retrieval provided by the OAuth Identity Provider.Refer to the RFC 6749 (http://tools.ietf.org/html/
rfc6749#section-3.2), section 3.2.",
      "propertyOrder" : 400,
      "type" : "string",
      "exampleValue" : ""
    },
```

```
   "authorizeEndpoint" : {
     "title" : "Authentication Endpoint URL",
     "description" : "OAuth authentication endpoint URL <p> This is the URL endpoint for OAuth
authentication provided by the OAuth Identity Provider.",
     "propertyOrder" : 300,
     "type" : "string",
     "exampleValue" : ""
   },
   "openIdValidationValue" : {
     "title" : "OpenID Connect Validation Value",
     "description" : "Specifies the full URL to the discovery or JWK location, corresponding to
the configuration type selected in the OpenID Connect validation configuration type property. <p>
Example: https://accounts.google.com/.well-known/openid-configuration",
     "propertyOrder" : 2000,
     "type" : "string",
     "exampleValue" : ""
   },
   "cfgAccountProviderClass" : {
     "title" : "Account Provider",
     "description" : "Name of the class implementing the account provider. This class
is used by the node to find the account from the attributes mapped by the Account Mapper
<code>org.forgerock.openam.authentication.modules.common.mapping.AccountProvider</code> interface.
String constructor parameters can be provided by appending | separated values.",
     "propertyOrder" : 1100,
     "type" : "string",
     "exampleValue" : ""
   },
   "userInfoEndpoint" : {
     "title" : "User Profile Service URL",
     "description" : "User profile information URL <p> This URL endpoint provides user profile
information and is provided by the OAuth Identity Provider NB This URL should return JSON objects
in response <p> If this field is left empty, attributes will be mapped from claims returned on the
id_token and no call to the UserInfo endpoint will be made.",
     "propertyOrder" : 500,
     "type" : "string",
     "exampleValue" : ""
   },
   "scopeString" : {
     "title" : "OAuth Scope",
     "description" : "List of user profile properties<p>According to the OAuth 2.0 Authorization
Framework, scope is a space-separated list of user profile attributes that the client application
requires. The list depends on the permissions that the resource owner grants to the client
application. Some authorization servers use non-standard separators for scopes.",
     "propertyOrder" : 600,
     "type" : "string",
     "exampleValue" : ""
   },
   "clientId" : {
     "title" : "Client ID",
     "description" : "OAuth client_id parameter<p> For more information on the OAuth client_id
parameter refer to the RFC 6749 (http://tools.ietf.org/html/rfc6749#section-2.3.1), section 2.3.1.",
     "propertyOrder" : 100,
     "type" : "string",
     "exampleValue" : ""
   },
   "cfgAccountMapperConfiguration" : {
     "title" : "Account Mapper Configuration",
```

```
     "description" : "Mapping of OAuth account to local OpenAM account Attribute configuration that
will be used to map the account of the user authenticated in the OAuth 2.0 Provider to the local data
store in the OpenAM. Example: <code>OAuth2.0_attribute=local_attribute</code>",
     "propertyOrder" : 1400,
     "patternProperties" : {
       ".*" : {
         "type" : "string"
       }
     },
     "type" : "object",
     "exampleValue" : ""
   },
   "saveUserAttributesToSession" : {
     "title" : "Save Attributes in the Session",
     "description" : "If this option is enabled, the attributes configured in the attribute mapper
will be saved into the OpenAM session.",
     "propertyOrder" : 1600,
     "type" : "boolean",
     "exampleValue" : ""
   },
   "cfgAttributeMappingClasses" : {
     "title" : "Attribute Mapper",
     "description" : "Name of the class that implements the attribute
mapping This class maps the OAuth properties into OpenAM properties. A custom
attribute mapper can be provided. A custom attribute mapper must implement the
org.forgerock.openam.authentication.modules.common.mapping.AttributeMapper interface. Provided
implementations are: org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper
org.forgerock.openam.authentication.modules.oidc.JwtAttributeMapper (can only be used when using the
openid scope)",
     "propertyOrder" : 1300,
     "items" : {
       "type" : "string"
     },
     "minItems" : 1,
     "type" : "array",
     "exampleValue" : ""
   },
   "redirectURI" : {
     "title" : "Redirect URL",
     "description" : "",
     "propertyOrder" : 700,
     "type" : "string",
     "exampleValue" : ""
   },
   "basicAuth" : {
     "title" : "Use Basic Auth",
     "description" : "When enabled, the client will use basic auth for authenticating with the social
auth provider. Enabled by default.",
     "propertyOrder" : 1000,
     "type" : "boolean",
     "exampleValue" : ""
   },
   "clientSecret" : {
     "title" : "Client Secret",
     "description" : "OAuth client_secret parameter <p>For more information on the OAuth client_id
parameter refer to the RFC 6749 (http://tools.ietf.org/html/rfc6749#section-2.3.1), section 2.3.1.",
     "propertyOrder" : 200,
     "type" : "string",
     "format" : "password",
```

```
      "exampleValue" : ""
    }
  },
  "required" : [ "clientSecret", "cfgAttributeMappingConfiguration", "basicAuth", "userInfoEndpoint",
 "cfgMixUpMitigation", "redirectURI", "authenticationIdKey", "cfgAccountMapperClass",
 "openIdValidationMethod", "issuer", "provider", "saveUserAttributesToSession",
 "cfgAttributeMappingClasses", "clientId", "authorizeEndpoint", "tokenEndpoint",
 "cfgAccountProviderClass", "openIdValidationValue", "scopeString", "cfgAccountMapperConfiguration" ]
}
```

delete

Usage:

```
am> delete OpenIDConnect --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action OpenIDConnect --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action OpenIDConnect --realm Realm --actionName getCreatableTypes
```

listOutcomes

List the available outcomes for the node type.

Usage:

```
am> action OpenIDConnect --realm Realm --body body --actionName listOutcomes
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "title" : "Some configuration of the node. This does not need to be complete against the
 configuration schema."
}
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action OpenIDConnect --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query OpenIDConnect --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read OpenIDConnect --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update OpenIDConnect --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "cfgMixUpMitigation" : {
      "title" : "OAuth 2.0 Mix-Up Mitigation Enabled",
      "description" : "Enables OAuth 2.0 mix-up mitigation The authorization server must support
 the OAuth 2.0 Mix-Up Mitigation draft (https://tools.ietf.org/html/draft-ietf-oauth-mix-up-
mitigation-01#section-3.1), otherwise OpenAM will fail to validate responses from the authorization
 server. If only the OAuth 2.0 protocol is utilized, make sure that the accepted issuer value is set
 in the \"Token Issuer\" setting.",
      "propertyOrder" : 1700,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "openIdValidationMethod" : {
      "title" : "OpenID Connect Validation Type",
      "description" : "In order to validate the ID token from the OpenID Connect provider, the node
 needs either a URL to get the public keys for the provider, or the symmetric key for an ID token
 signed with a HMAC-based algorithm. <p> By default, the configuration type is .well-known/openid-
configuration_url. This means the node should retrieve the keys based on information in the OpenID
 Connect Provider Configuration Document. <p>You can instead configure the authentication node to
 validate the ID token signature with the client secret key you provide, or to validate the ID token
 with the keys retrieved from the URL to the OpenID Connect provider's JSON web key set.",
      "propertyOrder" : 1900,
      "type" : "string",
      "exampleValue" : ""
    },
    "cfgAttributeMappingConfiguration" : {
      "title" : "Attribute Mapper Configuration",
      "description" : "Mapping of OAuth attributes to local OpenAM attributes Attribute configuration
 that will be used to map the user info obtained from the OAuth 2.0 Provider to the local user data
 store in the OpenAM. Example: OAuth2.0_attribute=local_attribute",
      "propertyOrder" : 1500,
      "patternProperties" : {
        ".*" : {
          "type" : "string"
        }
      },
      "type" : "object",
      "exampleValue" : ""
    },
    "provider" : {
      "title" : "Social Provider",
      "description" : "Social Provider for which this node is being setup.",
      "propertyOrder" : 800,
      "type" : "string",
      "exampleValue" : ""
    },
    "authenticationIdKey" : {
      "title" : "Auth ID Key",
      "description" : "",
```

```
      "propertyOrder" : 900,
      "type" : "string",
      "exampleValue" : ""
    },
    "issuer" : {
      "title" : "Token Issuer",
      "description" : "Required when the 'openid' scope is included. Value must match the iss field in
 issued ID Token e.g. <code>accounts.google.com</code> The issuer value MUST be provided when OAuth
 2.0 Mix-Up Mitigation is enabled.",
      "propertyOrder" : 1800,
      "type" : "string",
      "exampleValue" : ""
    },
    "cfgAccountMapperClass" : {
      "title" : "Account Mapper",
      "description" : "Name of the class implementing the attribute mapping for the
 account search. This class is used by the node to map from the account information
 received from the OAuth Identity Provider into OpenAM. The class must implement the
 <code>org.forgerock.openam.authentication.modules.common.mapping.AttributeMapper</code> interface.
 Provided implementations are:
 <code>org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper
 org.forgerock.openam.authentication.modules.oidc.JwtAttributeMapper</code> (canonly be used when
 using the openid scope) String constructor parameters can be provided by appending | separated
 values.",
      "propertyOrder" : 1200,
      "type" : "string",
      "exampleValue" : ""
    },
    "tokenEndpoint" : {
      "title" : "Access Token Endpoint URL",
      "description" : "OAuth access token endpoint URL This is the URL endpoint for access token
 retrieval provided by the OAuth Identity Provider.Refer to the RFC 6749 (http://tools.ietf.org/html/
rfc6749#section-3.2), section 3.2.",
      "propertyOrder" : 400,
      "type" : "string",
      "exampleValue" : ""
    },
    "authorizeEndpoint" : {
      "title" : "Authentication Endpoint URL",
      "description" : "OAuth authentication endpoint URL <p> This is the URL endpoint for OAuth
 authentication provided by the OAuth Identity Provider.",
      "propertyOrder" : 300,
      "type" : "string",
      "exampleValue" : ""
    },
    "openIdValidationValue" : {
      "title" : "OpenID Connect Validation Value",
      "description" : "Specifies the full URL to the discovery or JWK location, corresponding to
 the configuration type selected in the OpenID Connect validation configuration type property. <p>
 Example: https://accounts.google.com/.well-known/openid-configuration",
      "propertyOrder" : 2000,
      "type" : "string",
      "exampleValue" : ""
    },
    "cfgAccountProviderClass" : {
      "title" : "Account Provider",
      "description" : "Name of the class implementing the account provider. This class
 is used by the node to find the account from the attributes mapped by the Account Mapper
```

```
<code>org.forgerock.openam.authentication.modules.common.mapping.AccountProvider</code> interface.
String constructor parameters can be provided by appending | separated values.",
     "propertyOrder" : 1100,
     "type" : "string",
     "exampleValue" : ""
   },
   "userInfoEndpoint" : {
     "title" : "User Profile Service URL",
     "description" : "User profile information URL <p> This URL endpoint provides user profile
information and is provided by the OAuth Identity Provider NB This URL should return JSON objects
in response <p> If this field is left empty, attributes will be mapped from claims returned on the
id_token and no call to the UserInfo endpoint will be made.",
     "propertyOrder" : 500,
     "type" : "string",
     "exampleValue" : ""
   },
   "scopeString" : {
     "title" : "OAuth Scope",
     "description" : "List of user profile properties<p>According to the OAuth 2.0 Authorization
Framework, scope is a space-separated list of user profile attributes that the client application
requires. The list depends on the permissions that the resource owner grants to the client
application. Some authorization servers use non-standard separators for scopes.",
     "propertyOrder" : 600,
     "type" : "string",
     "exampleValue" : ""
   },
   "clientId" : {
     "title" : "Client ID",
     "description" : "OAuth client_id parameter<p> For more information on the OAuth client_id
parameter refer to the RFC 6749 (http://tools.ietf.org/html/rfc6749#section-2.3.1), section 2.3.1.",
     "propertyOrder" : 100,
     "type" : "string",
     "exampleValue" : ""
   },
   "cfgAccountMapperConfiguration" : {
     "title" : "Account Mapper Configuration",
     "description" : "Mapping of OAuth account to local OpenAM account Attribute configuration that
will be used to map the account of the user authenticated in the OAuth 2.0 Provider to the local data
store in the OpenAM. Example: <code>OAuth2.0_attribute=local_attribute</code>",
     "propertyOrder" : 1400,
     "patternProperties" : {
       ".*" : {
         "type" : "string"
       }
     },
     "type" : "object",
     "exampleValue" : ""
   },
   "saveUserAttributesToSession" : {
     "title" : "Save Attributes in the Session",
     "description" : "If this option is enabled, the attributes configured in the attribute mapper
will be saved into the OpenAM session.",
     "propertyOrder" : 1600,
     "type" : "boolean",
     "exampleValue" : ""
   },
   "cfgAttributeMappingClasses" : {
     "title" : "Attribute Mapper",
```

```
      "description" : "Name of the class that implements the attribute
 mapping This class maps the OAuth properties into OpenAM properties. A custom
 attribute mapper can be provided. A custom attribute mapper must implement the
 org.forgerock.openam.authentication.modules.common.mapping.AttributeMapper interface. Provided
 implementations are: org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper
 org.forgerock.openam.authentication.modules.oidc.JwtAttributeMapper (can only be used when using the
 openid scope)",
      "propertyOrder" : 1300,
      "items" : {
        "type" : "string"
      },
      "minItems" : 1,
      "type" : "array",
      "exampleValue" : ""
    },
    "redirectURI" : {
      "title" : "Redirect URL",
      "description" : "",
      "propertyOrder" : 700,
      "type" : "string",
      "exampleValue" : ""
    },
    "basicAuth" : {
      "title" : "Use Basic Auth",
      "description" : "When enabled, the client will use basic auth for authenticating with the social
 auth provider. Enabled by default.",
      "propertyOrder" : 1000,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "clientSecret" : {
      "title" : "Client Secret",
      "description" : "OAuth client_secret parameter <p>For more information on the OAuth client_id
 parameter refer to the RFC 6749 (http://tools.ietf.org/html/rfc6749#section-2.3.1), section 2.3.1.",
      "propertyOrder" : 200,
      "type" : "string",
      "format" : "password",
      "exampleValue" : ""
    }
  },
  "required" : [ "clientSecret", "cfgAttributeMappingConfiguration", "basicAuth", "userInfoEndpoint",
 "cfgMixUpMitigation", "redirectURI", "authenticationIdKey", "cfgAccountMapperClass",
 "openIdValidationMethod", "issuer", "provider", "saveUserAttributesToSession",
 "cfgAttributeMappingClasses", "clientId", "authorizeEndpoint", "tokenEndpoint",
 "cfgAccountProviderClass", "openIdValidationValue", "scopeString", "cfgAccountMapperConfiguration" ]
}
```


OpenIdConnectModule

Realm Operations

Resource path: `/realm-config/authentication/modules/openidconnect`

Resource version: `1.0`

create

Usage:

```
am> create OpenIdConnectModule --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "cryptoContextType" : {
      "title" : "OpenID Connect validation configuration type",
      "description" : "Please select either 1. the issuer discovery url, 2. the issuer jwk url, or 3.
 the client_secret.",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "principalMapperClass" : {
      "title" : "Principal mapper class",
      "description" : "Class which implements mapping of jwt state to a Principal in
 the local identity repository<br><br>Any custom implementation must implement the
 <code>org.forgerock.openam.authentication.modules.common.mapping.AttributeMapper</code> interface.",
      "propertyOrder" : 900,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "idTokenIssuer" : {
      "title" : "Name of OpenID Connect ID Token Issuer",
      "description" : "Value must match the iss field in issued ID Token",
      "propertyOrder" : 500,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "audienceName" : {
      "title" : "Audience name",
      "description" : "A case sensitive string<br><br>The audience name for this OpenID Connect
 module. This will be used to check that the ID token received is intended for this module as an
 audience.",
      "propertyOrder" : 700,
      "required" : true,
      "type" : "string",
```

```
      "exampleValue" : ""
    },
    "useSubClaimIfNoMatch" : {
      "title" : "Use \"sub\" claim if no match",
      "description" : "If no account is found that matches, whether to use the \"sub\" claim as the
 principal name or (if false) to fail.",
      "propertyOrder" : 1000,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "cryptoContextValue" : {
      "title" : "OpenID Connect validation configuration value",
      "description" : "The discovery url, or jwk url, or the client_secret, corresponding to the
 selection above.<br><br>If discovery or jwk url entered, entry must be in valid url format, <br/>e.g.
 https://accounts.google.com/.well-known/openid-configuration<br/><i>NB </i>If client_secret entered,
 entry is ignored and the value of the Client Secret is used.",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "accountProviderClass" : {
      "title" : "Account provider class",
      "description" : "Name of the class implementing the account provider.<br><br>This class
 is used by the module to find the account from the attributes mapped by the Account Mapper
 <code>org.forgerock.openam.authentication.modules.common.mapping.AccountProvider</code> interface.",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "clientSecret" : {
      "title" : "Client Secret",
      "description" : "OAuth client_secret parameter<br><br>For more information on the OAuth
 client_secret parameter refer to the <a href=\"http://tools.ietf.org/html/rfc6749#section-2.3.1\"
 target=\"_blank\">RFC 6749</a>, section 2.3.1",
      "propertyOrder" : 301,
      "required" : true,
      "type" : "string",
      "format" : "password",
      "exampleValue" : ""
    },
    "jwtToLdapAttributeMappings" : {
      "title" : "Mapping of jwt attributes to local LDAP attributes",
      "description" : "Format: jwt_attribute=local_ldap_attribute<br><br>Mappings allow jwt entries to
 drive principal lookup. This entry determines how to translate between local LDAP attributes and the
 entries in the jwt. See <a href=\"http://openid.net/specs/openid-connect-core-1_0.html#ScopeClaims
\" target=\"_blank\">OpenID Connect Core 1.0 Specification</a> section 5.4 on how to request the
 inclusion of additional attributes in issued ID Tokens.",
      "propertyOrder" : 600,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "minItems" : 1,
      "type" : "array",
      "exampleValue" : ""
    },
```

```
    "acceptedAuthorizedParties" : {
      "title" : "List of accepted authorized parties",
      "description" : "A list of case sensitive strings which can be either string or URI
 values<br><br>A list of authorized parties which this module will accept ID tokens from. This will be
 checked against the authorized party claim of the ID token.",
      "propertyOrder" : 800,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "minItems" : 1,
      "type" : "array",
      "exampleValue" : ""
    },
    "idTokenHeaderName" : {
      "title" : "Name of header referencing the ID Token",
      "description" : "",
      "propertyOrder" : 400,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
```

delete

Usage:

```
am> delete OpenIdConnectModule --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action OpenIdConnectModule --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action OpenIdConnectModule --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action OpenIdConnectModule --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query OpenIdConnectModule --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read OpenIdConnectModule --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update OpenIdConnectModule --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "cryptoContextType" : {
      "title" : "OpenID Connect validation configuration type",
      "description" : "Please select either 1. the issuer discovery url, 2. the issuer jwk url, or 3.
the client_secret.",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "principalMapperClass" : {
      "title" : "Principal mapper class",
      "description" : "Class which implements mapping of jwt state to a Principal in
the local identity repository<br><br>Any custom implementation must implement the
<code>org.forgerock.openam.authentication.modules.common.mapping.AttributeMapper</code> interface.",
      "propertyOrder" : 900,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "idTokenIssuer" : {
      "title" : "Name of OpenID Connect ID Token Issuer",
      "description" : "Value must match the iss field in issued ID Token",
      "propertyOrder" : 500,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "audienceName" : {
      "title" : "Audience name",
      "description" : "A case sensitive string<br><br>The audience name for this OpenID Connect
module. This will be used to check that the ID token received is intended for this module as an
audience.",
      "propertyOrder" : 700,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "useSubClaimIfNoMatch" : {
      "title" : "Use \"sub\" claim if no match",
      "description" : "If no account is found that matches, whether to use the \"sub\" claim as the
principal name or (if false) to fail.",
      "propertyOrder" : 1000,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "cryptoContextValue" : {
      "title" : "OpenID Connect validation configuration value",
      "description" : "The discovery url, or jwk url, or the client_secret, corresponding to the
selection above.<br><br>If discovery or jwk url entered, entry must be in valid url format, <br/>e.g.
https://accounts.google.com/.well-known/openid-configuration<br/><i>NB </i>If client_secret entered,
entry is ignored and the value of the Client Secret is used.",
```

```
      "propertyOrder" : 300,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "accountProviderClass" : {
      "title" : "Account provider class",
      "description" : "Name of the class implementing the account provider.<br><br>This class
 is used by the module to find the account from the attributes mapped by the Account Mapper
 <code>org.forgerock.openam.authentication.modules.common.mapping.AccountProvider</code> interface.",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "clientSecret" : {
      "title" : "Client Secret",
      "description" : "OAuth client_secret parameter<br><br>For more information on the OAuth
 client_secret parameter refer to the <a href=\"http://tools.ietf.org/html/rfc6749#section-2.3.1\"
 target=\"_blank\">RFC 6749</a>, section 2.3.1",
      "propertyOrder" : 301,
      "required" : true,
      "type" : "string",
      "format" : "password",
      "exampleValue" : ""
    },
    "jwtToLdapAttributeMappings" : {
      "title" : "Mapping of jwt attributes to local LDAP attributes",
      "description" : "Format: jwt_attribute=local_ldap_attribute<br><br>Mappings allow jwt entries to
 drive principal lookup. This entry determines how to translate between local LDAP attributes and the
 entries in the jwt. See <a href=\"http://openid.net/specs/openid-connect-core-1_0.html#ScopeClaims
\" target=\"_blank\">OpenID Connect Core 1.0 Specification</a> section 5.4 on how to request the
 inclusion of additional attributes in issued ID Tokens.",
      "propertyOrder" : 600,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "minItems" : 1,
      "type" : "array",
      "exampleValue" : ""
    },
    "acceptedAuthorizedParties" : {
      "title" : "List of accepted authorized parties",
      "description" : "A list of case sensitive strings which can be either string or URI
 values<br><br>A list of authorized parties which this module will accept ID tokens from. This will be
 checked against the authorized party claim of the ID token.",
      "propertyOrder" : 800,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "minItems" : 1,
      "type" : "array",
      "exampleValue" : ""
    },
    "idTokenHeaderName" : {
      "title" : "Name of header referencing the ID Token",
      "description" : "",
```

```
      "propertyOrder" : 400,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
```

Global Operations

Resource path: `/global-config/authentication/modules/openidconnect`

Resource version: `1.0`

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action OpenIdConnectModule --global --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action OpenIdConnectModule --global --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action OpenIdConnectModule --global --actionName nextdescendents
```

read

Usage:

```
am> read OpenIdConnectModule --global
```

update

Usage:

```
am> update OpenIdConnectModule --global --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "defaults" : {
      "properties" : {
        "accountProviderClass" : {
          "title" : "Account provider class",
          "description" : "Name of the class implementing the account provider.<br><br>This
 class is used by the module to find the account from the attributes mapped by the Account Mapper
 <code>org.forgerock.openam.authentication.modules.common.mapping.AccountProvider</code> interface.",
          "propertyOrder" : 100,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "audienceName" : {
          "title" : "Audience name",
          "description" : "A case sensitive string<br><br>The audience name for this OpenID Connect
 module. This will be used to check that the ID token received is intended for this module as an
 audience.",
          "propertyOrder" : 700,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "cryptoContextValue" : {
          "title" : "OpenID Connect validation configuration value",
          "description" : "The discovery url, or jwk url, or the client_secret, corresponding to the
 selection above.<br><br>If discovery or jwk url entered, entry must be in valid url format, <br/>e.g.
 https://accounts.google.com/.well-known/openid-configuration<br/><i>NB </i>If client_secret entered,
 entry is ignored and the value of the Client Secret is used.",
          "propertyOrder" : 300,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "idTokenIssuer" : {
          "title" : "Name of OpenID Connect ID Token Issuer",
          "description" : "Value must match the iss field in issued ID Token",
          "propertyOrder" : 500,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "acceptedAuthorizedParties" : {
          "title" : "List of accepted authorized parties",
          "description" : "A list of case sensitive strings which can be either string or URI
 values<br><br>A list of authorized parties which this module will accept ID tokens from. This will be
 checked against the authorized party claim of the ID token.",
          "propertyOrder" : 800,
```

```
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "minItems" : 1,
          "type" : "array",
          "exampleValue" : ""
        },
        "principalMapperClass" : {
          "title" : "Principal mapper class",
          "description" : "Class which implements mapping of jwt state to a Principal
 in the local identity repository<br><br>Any custom implementation must implement the
 <code>org.forgerock.openam.authentication.modules.common.mapping.AttributeMapper</code> interface.",
          "propertyOrder" : 900,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "cryptoContextType" : {
          "title" : "OpenID Connect validation configuration type",
          "description" : "Please select either 1. the issuer discovery url, 2. the issuer jwk url, or
 3. the client_secret.",
          "propertyOrder" : 200,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "jwtToLdapAttributeMappings" : {
          "title" : "Mapping of jwt attributes to local LDAP attributes",
          "description" : "Format: jwt_attribute=local_ldap_attribute<br><br>Mappings allow jwt
 entries to drive principal lookup. This entry determines how to translate between local LDAP
 attributes and the entries in the jwt. See <a href=\"http://openid.net/specs/openid-connect-
core-1_0.html#ScopeClaims\" target=\"_blank\">OpenID Connect Core 1.0 Specification</a> section 5.4 on
 how to request the inclusion of additional attributes in issued ID Tokens.",
          "propertyOrder" : 600,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "minItems" : 1,
          "type" : "array",
          "exampleValue" : ""
        },
        "useSubClaimIfNoMatch" : {
          "title" : "Use \"sub\" claim if no match",
          "description" : "If no account is found that matches, whether to use the \"sub\" claim as
 the principal name or (if false) to fail.",
          "propertyOrder" : 1000,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "clientSecret" : {
          "title" : "Client Secret",
          "description" : "OAuth client_secret parameter<br><br>For more information on the OAuth
 client_secret parameter refer to the <a href=\"http://tools.ietf.org/html/rfc6749#section-2.3.1\"
 target=\"_blank\">RFC 6749</a>, section 2.3.1",
          "propertyOrder" : 301,
          "required" : true,
```

```
          "type" : "string",
          "format" : "password",
          "exampleValue" : ""
        },
        "idTokenHeaderName" : {
          "title" : "Name of header referencing the ID Token",
          "description" : "",
          "propertyOrder" : 400,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      },
      "type" : "object",
      "title" : "Realm Defaults"
    }
  }
}
```

PageNode

Realm Operations

Resource path: `/realm-config/authentication/authenticationtrees/nodes/PageNode`

Resource version: `1.0`

create

Usage:

```
am> create PageNode --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "$schema" : "http://json-schema.org/draft-04/schema#",
  "type" : "object",
  "properties" : {
    "pageHeader" : {
      "propertyOrder" : 100,
      "type" : "object",
      "title" : "Page Header",
```

```
      "description" : "Localisation overrides - as key fill shortcut for language (first will be used
as default if not empty or \"Default header\" if empty), value is header for language defined by
key",
      "exampleValue" : "",
      "patternProperties" : {
        ".*" : {
          "type" : "string"
        }
      }
    },
    "pageDescription" : {
      "propertyOrder" : 200,
      "type" : "object",
      "title" : "Page Description",
      "description" : "Localisation overrides - as key fill shortcut for language (first will be used
as default if not empty or \"Default description\" if empty), value is description for language
defined by key",
      "exampleValue" : "",
      "patternProperties" : {
        ".*" : {
          "type" : "string"
        }
      }
    },
    "stage" : {
      "propertyOrder" : 300,
      "type" : "string",
      "title" : "Stage",
      "description" : "An optional stage name to pass to the client to aid in rendering"
    },
    "nodes" : {
      "propertyOrder" : 400,
      "type" : "array",
      "title" : "Page Nodes",
      "description" : "The child nodes, in the order they are returned to the authentication client",
      "items" : {
        "type" : "object",
        "title" : "Child Node",
        "description" : "A node that is used in the page",
        "properties" : {
          "id" : {
            "type" : "string",
            "title" : "Node ID",
            "description" : "ID of the child node"
          },
          "displayName" : {
            "type" : "string",
            "title" : "Display name",
            "description" : "The display name of the child node"
          },
          "nodeType" : {
            "type" : "string",
            "title" : "Node type",
            "description" : "The type of the child node"
          }
        }
      }
    }
  },
```

```
  "required" : [ "nodes" ]
}
```

delete

Usage:

```
am> delete PageNode --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action PageNode --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action PageNode --realm Realm --actionName getCreatableTypes
```

listOutcomes

List the available outcomes for the node type.

Usage:

```
am> action PageNode --realm Realm --body body --actionName listOutcomes
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "title" : "Some configuration of the node. This does not need to be complete against the
 configuration schema."
}
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action PageNode --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query PageNode --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read PageNode --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update PageNode --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "$schema" : "http://json-schema.org/draft-04/schema#",
  "type" : "object",
  "properties" : {
    "pageHeader" : {
      "propertyOrder" : 100,
      "type" : "object",
      "title" : "Page Header",
      "description" : "Localisation overrides - as key fill shortcut for language (first will be used
 as default if not empty or \"Default header\" if empty), value is header for language defined by
 key",
      "exampleValue" : "",
      "patternProperties" : {
        ".*" : {
          "type" : "string"
        }
      }
    },
    "pageDescription" : {
      "propertyOrder" : 200,
      "type" : "object",
      "title" : "Page Description",
      "description" : "Localisation overrides - as key fill shortcut for language (first will be used
 as default if not empty or \"Default description\" if empty), value is description for language
 defined by key",
      "exampleValue" : "",
      "patternProperties" : {
        ".*" : {
          "type" : "string"
        }
      }
    },
    "stage" : {
      "propertyOrder" : 300,
      "type" : "string",
      "title" : "Stage",
      "description" : "An optional stage name to pass to the client to aid in rendering"
    },
    "nodes" : {
      "propertyOrder" : 400,
      "type" : "array",
      "title" : "Page Nodes",
      "description" : "The child nodes, in the order they are returned to the authentication client",
      "items" : {
        "type" : "object",
        "title" : "Child Node",
        "description" : "A node that is used in the page",
        "properties" : {
          "id" : {
            "type" : "string",
            "title" : "Node ID",
            "description" : "ID of the child node"
          },
          "displayName" : {
            "type" : "string",
```

```
            "title" : "Display name",
            "description" : "The display name of the child node"
          },
          "nodeType" : {
            "type" : "string",
            "title" : "Node type",
            "description" : "The type of the child node"
          }
        }
      }
    }
  },
  "required" : [ "nodes" ]
}
```

PasswordCollector

Realm Operations

Resource path: `/realm-config/authentication/authenticationtrees/nodes/PasswordCollectorNode`

Resource version: `1.0`

create

Usage:

```
am> create PasswordCollector --realm Realm --id id --body body
```

Parameters:

`--id`

The unique identifier for the resource.

`--body`

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "required" : [ ]
}
```

delete

Usage:

```
am> delete PasswordCollector --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action PasswordCollector --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action PasswordCollector --realm Realm --actionName getCreatableTypes
```

listOutcomes

List the available outcomes for the node type.

Usage:

```
am> action PasswordCollector --realm Realm --body body --actionName listOutcomes
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "title" : "Some configuration of the node. This does not need to be complete against the
 configuration schema."
}
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action PasswordCollector --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query PasswordCollector --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read PasswordCollector --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update PasswordCollector --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "required" : [ ]
}
```

PatchObject

Realm Operations

Resource path: `/realm-config/authentication/authenticationtrees/nodes/PatchObjectNode`

Resource version: `1.0`

create

Usage:

```
am> create PatchObject --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "patchAsObject" : {
      "title" : "Patch As Object",
      "description" : "Whether the patch should be done as object or client. Defaults to false, which
 represents the oauth client.",
      "propertyOrder" : 100,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "identityResource" : {
      "title" : "Identity Resource",
      "description" : "The identity resource in IDM that this node will patch. This is used to aid
 node input requirement declaration.  Must match identity resource of the current tree.",
      "propertyOrder" : 300,
      "type" : "string",
      "exampleValue" : ""
    },
    "ignoredFields" : {
      "title" : "Ignored Fields",
      "description" : "Fields from sharedState that should be ignored as part of patch. If empty, all
 fields are attempted as part of the patch.",
      "propertyOrder" : 200,
      "items" : {
        "type" : "string"
```

```
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "identityAttribute" : {
      "title" : "Identity Attribute",
      "description" : "The attribute used to identify the the object in IDM.",
      "propertyOrder" : 400,
      "type" : "string",
      "exampleValue" : ""
    }
  },
  "required" : [ "identityAttribute", "ignoredFields", "identityResource", "patchAsObject" ]
}
```

delete

Usage:

```
am> delete PatchObject --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action PatchObject --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action PatchObject --realm Realm --actionName getCreatableTypes
```

listOutcomes

List the available outcomes for the node type.

Usage:

```
am> action PatchObject --realm Realm --body body --actionName listOutcomes
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "title" : "Some configuration of the node. This does not need to be complete against the
 configuration schema."
}
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action PatchObject --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query PatchObject --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read PatchObject --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update PatchObject --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "patchAsObject" : {
      "title" : "Patch As Object",
      "description" : "Whether the patch should be done as object or client. Defaults to false, which
 represents the oauth client.",
      "propertyOrder" : 100,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "identityResource" : {
      "title" : "Identity Resource",
      "description" : "The identity resource in IDM that this node will patch. This is used to aid
 node input requirement declaration.  Must match identity resource of the current tree.",
      "propertyOrder" : 300,
      "type" : "string",
      "exampleValue" : ""
    },
    "ignoredFields" : {
      "title" : "Ignored Fields",
      "description" : "Fields from sharedState that should be ignored as part of patch. If empty, all
 fields are attempted as part of the patch.",
      "propertyOrder" : 200,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "identityAttribute" : {
      "title" : "Identity Attribute",
      "description" : "The attribute used to identify the the object in IDM.",
      "propertyOrder" : 400,
      "type" : "string",
      "exampleValue" : ""
    }
  },
  "required" : [ "identityAttribute", "ignoredFields", "identityResource", "patchAsObject" ]
```

```
}
```

PendingUmaRequests

Realm Operations

Pending UMA requests provider is responsible for allowing, denying and querying the guest requests for user resources. Awailable actions are Query, Read, Deny (all requests or one request), Approve (all requests or one request)

Resource path: `/users/{user}/uma/pendingrequests`

Resource version: `1.0`

approve

Approve the pending request and grant access to the requesting user.

Usage:

```
am> action PendingUmaRequests --realm Realm --id id --body body --user user --actionName approve
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "$schema" : "http://json-schema.org/draft-04/schema#",
  "description" : "Approve action request schema.",
  "type" : "object",
  "title" : "Approve action request schema",
  "properties" : {
    "scopes" : {
      "type" : "array",
      "title" : "Approve request scopes",
      "description" : "The list of the scopes the requesting user gets access to.",
      "items" : {
        "type" : "string"
      }
    }
  },
  "required" : [ "scopes" ]
}
```

--user

Pending UMA requests provider is responsible for allowing, denying and querying the guest requests for user resources. Available actions are Query, Read, Deny (all requests or one request), Approve (all requests or one request)

approveAll

Approve every pending requests and grant access to the requesting user.

Usage:

```
am> action PendingUmaRequests --realm Realm --body body --user user --actionName approveAll
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "$schema" : "http://json-schema.org/draft-04/schema#",
  "description" : "Approve action request schema.",
  "type" : "object",
  "title" : "Approve action request schema",
  "properties" : {
    "scopes" : {
      "type" : "array",
      "title" : "Approve request scopes",
      "description" : "The list of the scopes the requesting user gets access to.",
      "items" : {
        "type" : "string"
      }
    }
  },
  "required" : [ "scopes" ]
}
```

--user

Pending UMA requests provider is responsible for allowing, denying and querying the guest requests for user resources. Available actions are Query, Read, Deny (all requests or one request), Approve (all requests or one request)

query

Query the collection of pending requests.

Usage:

```
am> query PendingUmaRequests --realm Realm --filter filter --user user
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all. Fields that can be queried: [*]

--user

Pending UMA requests provider is responsible for allowing, denying and querying the guest requests for user resources. Available actions are Query, Read, Deny (all requests or one request), Approve (all requests or one request)

read

Read pending request

Usage:

```
am> read PendingUmaRequests --realm Realm --id id --user user
```

Parameters:

--id

The unique identifier for the resource.

--user

Pending UMA requests provider is responsible for allowing, denying and querying the guest requests for user resources. Available actions are Query, Read, Deny (all requests or one request), Approve (all requests or one request)

PersistentCookieDecision

Realm Operations

Resource path: `/realm-config/authentication/authenticationtrees/nodes/PersistentCookieDecisionNode`

Resource version: `1.0`

create

Usage:

```
am> create PersistentCookieDecision --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "useSecureCookie" : {
      "title" : "Use Secure Cookie",
      "description" : "Sets the persistent cookie as \"Secure\".",
      "propertyOrder" : 300,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "useHttpOnlyCookie" : {
      "title" : "Use HTTP Only Cookie",
      "description" : "Sets the persistent cookie as \"HttpOnly\".",
      "propertyOrder" : 400,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "enforceClientIp" : {
      "title" : "Enforce Client IP",
      "description" : "Enforces that the persistent cookie can only be used from the same client IP to
 which the cookie was issued.",
      "propertyOrder" : 200,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "persistentCookieName" : {
      "title" : "Persistent Cookie Name",
      "description" : "The name of the persistent cookie.",
      "propertyOrder" : 600,
      "type" : "string",
      "exampleValue" : ""
    },
    "hmacSigningKey" : {
      "title" : "HMAC Signing Key",
      "description" : "Base64-encoded 256-bit key to use for HMAC signing of the cookie.",
      "propertyOrder" : 500,
      "type" : "string",
      "format" : "password",
      "exampleValue" : ""
    },
    "idleTimeout" : {
      "title" : "Idle Timeout",
      "description" : "The maximum idle time between requests before the cookie is invalidated, in
 hours.",
      "propertyOrder" : 100,
```

```
      "type" : "integer",
      "exampleValue" : ""
    }
  },
  "required" : [ "hmacSigningKey", "useHttpOnlyCookie", "idleTimeout", "persistentCookieName",
 "enforceClientIp", "useSecureCookie" ]
}
```

delete

Usage:

```
am> delete PersistentCookieDecision --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action PersistentCookieDecision --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action PersistentCookieDecision --realm Realm --actionName getCreatableTypes
```

listOutcomes

List the available outcomes for the node type.

Usage:

```
am> action PersistentCookieDecision --realm Realm --body body --actionName listOutcomes
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "title" : "Some configuration of the node. This does not need to be complete against the
 configuration schema."
}
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action PersistentCookieDecision --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query PersistentCookieDecision --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read PersistentCookieDecision --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update PersistentCookieDecision --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "useSecureCookie" : {
      "title" : "Use Secure Cookie",
      "description" : "Sets the persistent cookie as \"Secure\".",
      "propertyOrder" : 300,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "useHttpOnlyCookie" : {
      "title" : "Use HTTP Only Cookie",
      "description" : "Sets the persistent cookie as \"HttpOnly\".",
      "propertyOrder" : 400,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "enforceClientIp" : {
      "title" : "Enforce Client IP",
      "description" : "Enforces that the persistent cookie can only be used from the same client IP to
 which the cookie was issued.",
      "propertyOrder" : 200,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "persistentCookieName" : {
      "title" : "Persistent Cookie Name",
      "description" : "The name of the persistent cookie.",
      "propertyOrder" : 600,
      "type" : "string",
      "exampleValue" : ""
    },
    "hmacSigningKey" : {
      "title" : "HMAC Signing Key",
      "description" : "Base64-encoded 256-bit key to use for HMAC signing of the cookie.",
      "propertyOrder" : 500,
      "type" : "string",
      "format" : "password",
      "exampleValue" : ""
    },
    "idleTimeout" : {
      "title" : "Idle Timeout",
      "description" : "The maximum idle time between requests before the cookie is invalidated, in
 hours.",
      "propertyOrder" : 100,
      "type" : "integer",
      "exampleValue" : ""
    }
```

```
  },
  "required" : [ "hmacSigningKey", "useHttpOnlyCookie", "idleTimeout", "persistentCookieName",
 "enforceClientIp", "useSecureCookie" ]
}
```

PersistentCookieModule

Realm Operations

Resource path: `/realm-config/authentication/modules/persistentcookie`

Resource version: `1.0`

create

Usage:

```
am> create PersistentCookieModule --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "cookieName" : {
      "title" : "Persistent Cookie Name",
      "description" : "Sets the name of the persistent cookie",
      "propertyOrder" : null,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "idleTimeout" : {
      "title" : "Idle Timeout",
      "description" : "The maximum idle time between requests before the cookie is invalidated, in
 hours.",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "maxLife" : {
```

```
      "title" : "Max Life",
      "description" : "The maximum length of time the persistent cookie is valid for, in hours.",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "useSecureCookie" : {
      "title" : "Use secure cookie",
      "description" : "Sets the persistent cookie as \"Secure\"",
      "propertyOrder" : 400,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "enforceClientIP" : {
      "title" : "Enforce Client IP",
      "description" : "Enforces that the persistent cookie can only be used from the same client IP to
 which the cookie was issued.",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "useHttpOnlyCookie" : {
      "title" : "Use HTTP only cookie",
      "description" : "Sets the persistent cookie as \"HttpOnly\"",
      "propertyOrder" : 500,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    }
  }
}
```

delete

Usage:

```
am> delete PersistentCookieModule --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action PersistentCookieModule --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action PersistentCookieModule --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action PersistentCookieModule --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query PersistentCookieModule --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read PersistentCookieModule --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update PersistentCookieModule --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "cookieName" : {
      "title" : "Persistent Cookie Name",
      "description" : "Sets the name of the persistent cookie",
      "propertyOrder" : null,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "idleTimeout" : {
      "title" : "Idle Timeout",
      "description" : "The maximum idle time between requests before the cookie is invalidated, in
 hours.",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "maxLife" : {
      "title" : "Max Life",
      "description" : "The maximum length of time the persistent cookie is valid for, in hours.",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "useSecureCookie" : {
      "title" : "Use secure cookie",
      "description" : "Sets the persistent cookie as \"Secure\"",
      "propertyOrder" : 400,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "enforceClientIP" : {
      "title" : "Enforce Client IP",
      "description" : "Enforces that the persistent cookie can only be used from the same client IP to
 which the cookie was issued.",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "useHttpOnlyCookie" : {
      "title" : "Use HTTP only cookie",
      "description" : "Sets the persistent cookie as \"HttpOnly\"",
      "propertyOrder" : 500,
      "required" : true,
      "type" : "boolean",
```

```
      "exampleValue" : ""
    }
  }
}
```

Global Operations

Resource path: `/global-config/authentication/modules/persistentcookie`

Resource version: `1.0`

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action PersistentCookieModule --global --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action PersistentCookieModule --global --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action PersistentCookieModule --global --actionName nextdescendents
```

read

Usage:

```
am> read PersistentCookieModule --global
```

update

Usage:

```
am> update PersistentCookieModule --global --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "defaults" : {
      "properties" : {
        "idleTimeout" : {
          "title" : "Idle Timeout",
          "description" : "The maximum idle time between requests before the cookie is invalidated, in
 hours.",
          "propertyOrder" : 100,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "maxLife" : {
          "title" : "Max Life",
          "description" : "The maximum length of time the persistent cookie is valid for, in hours.",
          "propertyOrder" : 200,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "cookieName" : {
          "title" : "Persistent Cookie Name",
          "description" : "Sets the name of the persistent cookie",
          "propertyOrder" : null,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "useSecureCookie" : {
          "title" : "Use secure cookie",
          "description" : "Sets the persistent cookie as \"Secure\"",
          "propertyOrder" : 400,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "enforceClientIP" : {
          "title" : "Enforce Client IP",
          "description" : "Enforces that the persistent cookie can only be used from the same client
 IP to which the cookie was issued.",
          "propertyOrder" : 300,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "useHttpOnlyCookie" : {
          "title" : "Use HTTP only cookie",
          "description" : "Sets the persistent cookie as \"HttpOnly\"",
          "propertyOrder" : 500,
          "required" : true,
          "type" : "boolean",
```

```
          "exampleValue" : ""
        }
      },
      "type" : "object",
      "title" : "Realm Defaults"
    }
  }
}
```

Platform

Global Operations

Resource path: `/global-config/services/platform`

Resource version: `1.0`

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action Platform --global --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action Platform --global --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action Platform --global --actionName nextdescendents
```

read

Usage:

```
am> read Platform --global
```

update

Usage:

```
am> update Platform --global --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "cookieDomains" : {
      "title" : "Cookie Domains",
      "description" : "Set the list of domains into which OpenAM writes cookies.<br><br>If you set
 multiple cookie domains, OpenAM still only sets the cookie in the domain the client uses to access
 OpenAM. If this property is left blank, then the fully qualified domain name of the server is used to
 set the cookie domain, meaning that a host cookie rather than a domain cookie is set.",
      "propertyOrder" : 200,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "locale" : {
      "title" : "Platform Locale",
      "description" : "Set the fallback locale used when the user locale cannot be determined.",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
```

PlatformPassword

Realm Operations

Resource path: `/realm-config/authentication/authenticationtrees/nodes/ValidatedPasswordNode`

Resource version: `1.0`

create

Usage:

```
am> create PlatformPassword --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "validateInput" : {
      "title" : "Validate password",
      "description" : "Check IDM policy against this password and return any policy failures as
 errors.",
      "propertyOrder" : 100,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "passwordAttribute" : {
      "title" : "Password Attribute",
      "description" : "The name of the attribute in the IDM object that stores the password.",
      "propertyOrder" : 200,
      "type" : "string",
      "exampleValue" : ""
    }
  },
  "required" : [ "validateInput", "passwordAttribute" ]
}
```

delete

Usage:

```
am> delete PlatformPassword --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action PlatformPassword --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action PlatformPassword --realm Realm --actionName getCreatableTypes
```

listOutcomes

List the available outcomes for the node type.

Usage:

```
am> action PlatformPassword --realm Realm --body body --actionName listOutcomes
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "title" : "Some configuration of the node. This does not need to be complete against the
 configuration schema."
}
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action PlatformPassword --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query PlatformPassword --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read PlatformPassword --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update PlatformPassword --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "validateInput" : {
      "title" : "Validate password",
      "description" : "Check IDM policy against this password and return any policy failures as
 errors.",
      "propertyOrder" : 100,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "passwordAttribute" : {
      "title" : "Password Attribute",
      "description" : "The name of the attribute in the IDM object that stores the password.",
      "propertyOrder" : 200,
      "type" : "string",
      "exampleValue" : ""
    }
  },
  "required" : [ "validateInput", "passwordAttribute" ]
}
```

PlatformUsername

Realm Operations

Resource path: `/realm-config/authentication/authenticationtrees/nodes/ValidatedUsernameNode`

Resource version: `1.0`

create

Usage:

```
am> create PlatformUsername --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "validateInput" : {
      "title" : "Validate username",
      "description" : "Check IDM policy against this username and return any policy failures as
 errors.",
      "propertyOrder" : 100,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "usernameAttribute" : {
      "title" : "Username Attribute",
      "description" : "The name of the attribute in the IDM object that stores the username.",
      "propertyOrder" : 200,
      "type" : "string",
      "exampleValue" : ""
    }
  },
  "required" : [ "usernameAttribute", "validateInput" ]
}
```

delete

Usage:

```
am> delete PlatformUsername --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action PlatformUsername --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action PlatformUsername --realm Realm --actionName getCreatableTypes
```

listOutcomes

List the available outcomes for the node type.

Usage:

```
am> action PlatformUsername --realm Realm --body body --actionName listOutcomes
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "title" : "Some configuration of the node. This does not need to be complete against the
 configuration schema."
}
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action PlatformUsername --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query PlatformUsername --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read PlatformUsername --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update PlatformUsername --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "validateInput" : {
      "title" : "Validate username",
      "description" : "Check IDM policy against this username and return any policy failures as
 errors.",
      "propertyOrder" : 100,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "usernameAttribute" : {
      "title" : "Username Attribute",
      "description" : "The name of the attribute in the IDM object that stores the username.",
      "propertyOrder" : 200,
      "type" : "string",
      "exampleValue" : ""
    }
  },
  "required" : [ "usernameAttribute", "validateInput" ]
}
```

Policies

Realm Operations

The Policy resource with copy and move support endpoint is responsible for managing policies. It supports all the operations that previous version of Policy resource endpoint supports - create, read, update, delete, query, evalute and evaluateTree action - with two new actions move and copy for copying and moving policies between realms

Resource path: `/policies`

Resource version: `2.1`

copy

Copy a list of policies

Usage:

```
am> action Policies --realm Realm --body body --actionName copy
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "$schema" : "http://json-schema.org/draft-04/schema#",
  "description" : "Policy copy action schema",
  "type" : "object",
  "title" : "Policy copy action schema",
  "properties" : {
    "from" : {
      "title" : "Copy/move from",
      "description" : "Policy copy/move origin parameters",
      "type" : "object",
      "properties" : {
        "application" : {
          "title" : "Application",
          "description" : "The policy set in which the input policies are located",
          "type" : "string"
        }
      },
      "required" : [ "application" ]
    },
    "to" : {
      "type" : "object",
      "title" : "Copy/Move To",
      "description" : "Policy copy/move destination parameters",
      "properties" : {
        "application" : {
          "title" : "Application",
```

```
          "description" : "The policy set in which to place the output policy. Required when copying
 or moving a policy to a different policy set.",
          "type" : "string"
        },
        "realm" : {
          "title" : "Realm",
          "description" : "The realm in which to place the output policy. If not specified, OpenAM
 copies or moves the policy within the realm identified in the URL. Required when copying or moving a
 policy to a different realm.",
          "type" : "string"
        },
        "namePostfix" : {
          "title" : "Name postfix",
          "description" : "A value appended to output policy names in order to prevent name clashes",
          "type" : "string"
        }
      },
      "required" : [ "namePostfix" ]
    },
    "resourceTypeMapping" : {
      "title" : "Resource type mapping",
      "description" : "One or more resource types mappings, where the left side of the mapping
 specifies the UUID of a resource type used by the input policies and the right side of the mapping
 specifies the UUID of a resource type used by the output policies. The two resource types should have
 the same resource patterns",
      "type" : "object",
      "additionalProperties" : {
        "type" : "string"
      }
    }
  },
  "required" : [ "from", "to" ]
}
```

create

Create new policy

Usage:

```
am> create Policies --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "$schema" : "http://json-schema.org/draft-04/schema#",
  "description" : "Json schema for the policy resource",
  "title" : "Policy Resource Schema",
  "type" : "object",
```

```
 "properties" : {
   "name" : {
     "title" : "Name",
     "description" : "String matching the name of the application",
     "type" : "string"
   },
   "active" : {
     "title" : "Active flag",
     "description" : "Boolean indicating whether OpenAM considers the policy active for evaluation
purposes, defaults to false",
     "type" : "boolean"
   },
   "description" : {
     "title" : "Description",
     "description" : "String describing the policy",
     "type" : "string"
   },
   "applicationName" : {
     "title" : "Application name",
     "description" : "String containing the application name, such as \"iPlanetAMWebAgentService\",
or \"mypolicyset\"",
     "type" : "string"
   },
   "actionValues" : {
     "title" : "Action values",
     "description" : "Set of string action names, each set to a boolean indicating whether the action
is allowed. Chosen from the available actions provided by the associated Managing Resource Types
resource type",
     "type" : "object",
     "additionalProperties" : {
       "type" : "boolean"
     }
   },
   "resources" : {
     "title" : "Resources",
     "description" : "List of the resource name pattern strings to which the policy applies. Must
conform to the pattern templates provided by the associated Managing Resource Types resource type",
     "type" : "array",
     "items" : {
       "type" : "string"
     }
   },
   "subject" : {
     "title" : "Subject",
     "description" : "Specifies the subject conditions to which the policy applies, where subjects
can be combined by using the built-in types \"AND\", \"OR\", and \"NOT\", and where subject
implementations are pluggable",
     "type" : "object"
   },
   "condition" : {
     "title" : "Condition",
     "description" : "Specifies environment conditions, where conditions can be combined by using the
built-in types \"AND\", \"OR\", and \"NOT\", and where condition implementations are pluggable",
     "type" : "object",
     "properties" : {
       "type" : {
         "type" : "string"
       },
       "conditions" : {
```

```
          "type" : "array",
          "title" : "Condition",
          "description" : "Specifies environment conditions, where conditions can be combined by using
 the built-in types \"AND\", \"OR\", and \"NOT\", and where condition implementations are pluggable",
          "items" : {
            "type" : "object"
          }
        }
      }
    },
    "resourceTypeUuid" : {
      "title" : "Resource Type UUID",
      "description" : "The UUIDs of the resource type associated with the policy",
      "type" : "string"
    },
    "resourceAttributes" : {
      "title" : "Resource Attributes",
      "description" : "List of attributes to return with decisions. These attributes are known as
 response attributes",
      "type" : "array",
      "items" : {
        "type" : "object"
      }
    },
    "lastModifiedBy" : {
      "title" : "Last Modified By",
      "description" : "A string containing the universal identifier DN of the subject that most
 recently updated the policy",
      "type" : "string"
    },
    "lastModifiedDate" : {
      "title" : "Last Modified date",
      "description" : "An integer containing the last modified date and time, in number of seconds",
      "type" : "string"
    },
    "createdBy" : {
      "title" : "Created By",
      "description" : "A string containing the universal identifier DN of the subject that created the
 policy",
      "type" : "string"
    },
    "creationDate" : {
      "title" : "Creation Date",
      "description" : "An integer containing the creation date and time, in number of seconds",
      "type" : "string"
    }
  }
}
```

delete

Delete policy

Usage:

```
am> delete Policies --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

evaluate

Request policy decisions for specific resources

Usage:

```
am> action Policies --realm Realm --body body --actionName evaluate
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "$schema" : "http://json-schema.org/draft-04/schema#",
  "description" : "Evaluate action schema",
  "title" : "Evaluate action schema",
  "type" : "object",
  "properties" : {
    "resources" : {
      "type" : "array",
      "title" : "Resources",
      "description" : "Specifies the list of resources for which to return decisions",
      "items" : {
        "type" : "string"
      }
    },
    "application" : {
      "title" : "Application",
      "description" : "Holds the name of the application, and defaults to \"iPlanetAMWebAgentService\"
 if not specified",
      "type" : "string"
    },
    "subject" : {
      "title" : "Subject",
      "description" : "Holds an object that represents the subject. You can specify one or more of the
 following keys. If you specify multiple keys, the subject can have multiple associated principals,
 and you can use subject conditions corresponding to any type in the request",
      "type" : "object",
      "properties" : {
        "ssoToken" : {
          "title" : "SSOToken",
          "description" : "The value is the SSO token ID string for the subject",
          "type" : "string"
        },
        "jwt" : {
          "title" : "JWT",
          "description" : "The value is a JWT string",
          "type" : "string"
        },
```

```
        "claims" : {
          "title" : "Claims",
          "description" : "The value is an object (map) of JWT claims to their values.",
          "type" : "object",
          "additionalProperties" : {
            "type" : "string"
          }
        }
      }
    },
    "environment" : {
      "title" : "Environment",
      "description" : "Holds a map of keys to lists of values",
      "type" : "object",
      "additionalProperties" : {
        "type" : "array",
        "items" : {
          "type" : "string"
        }
      }
    }
  },
  "required" : [ "resources", "application" ]
}
```

evaluateTree

Request policy decisions for a tree of resources

Usage:

```
am> action Policies --realm Realm --body body --actionName evaluateTree
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "$schema" : "http://json-schema.org/draft-04/schema#",
  "description" : "Evaluate tree action schema",
  "title" : "Evaluate tree action schema",
  "type" : "object",
  "properties" : {
    "resource" : {
      "title" : "Resource",
      "description" : "Specifies the root resource for the decisions to return",
      "type" : "string"
    },
    "application" : {
      "title" : "Application",
      "description" : "Holds the name of the application, and defaults to \"iPlanetAMWebAgentService\"
 if not specified",
      "type" : "string"
    },
    "subject" : {
```

```
      "title" : "Subject",
      "description" : "Holds an object that represents the subject. You can specify one or more of the
 following keys. If you specify multiple keys, the subject can have multiple associated principals,
 and you can use subject conditions corresponding to any type in the request",
      "type" : "object",
      "properties" : {
        "ssoToken" : {
          "title" : "SSOToken",
          "description" : "The value is the SSO token ID string for the subject",
          "type" : "string"
        },
        "jwt" : {
          "title" : "JWT",
          "description" : "The value is a JWT string",
          "type" : "string"
        },
        "claims" : {
          "title" : "Claims",
          "description" : "The value is an object (map) of JWT claims to their values.",
          "type" : "object",
          "additionalProperties" : {
            "type" : "string"
          }
        }
      }
    },
    "environment" : {
      "title" : "Environment",
      "description" : "Holds a map of keys to lists of values",
      "type" : "object",
      "additionalProperties" : {
        "type" : "array",
        "items" : {
          "type" : "string"
        }
      }
    }
  },
  "required" : [ "resources", "application" ]
}
```

move

Move a list of policies

Usage:

```
am> action Policies --realm Realm --body body --actionName move
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "$schema" : "http://json-schema.org/draft-04/schema#",
```

```
  "description" : "Policy copy action schema",
  "type" : "object",
  "title" : "Policy copy action schema",
  "properties" : {
    "from" : {
      "title" : "Copy/move from",
      "description" : "Policy copy/move origin parameters",
      "type" : "object",
      "properties" : {
        "application" : {
          "title" : "Application",
          "description" : "The policy set in which the input policies are located",
          "type" : "string"
        }
      },
      "required" : [ "application" ]
    },
    "to" : {
      "type" : "object",
      "title" : "Copy/Move To",
      "description" : "Policy copy/move destination parameters",
      "properties" : {
        "application" : {
          "title" : "Application",
          "description" : "The policy set in which to place the output policy. Required when copying
 or moving a policy to a different policy set.",
          "type" : "string"
        },
        "realm" : {
          "title" : "Realm",
          "description" : "The realm in which to place the output policy. If not specified, OpenAM
 copies or moves the policy within the realm identified in the URL. Required when copying or moving a
 policy to a different realm.",
          "type" : "string"
        },
        "namePostfix" : {
          "title" : "Name postfix",
          "description" : "A value appended to output policy names in order to prevent name clashes",
          "type" : "string"
        }
      },
      "required" : [ "namePostfix" ]
    },
    "resourceTypeMapping" : {
      "title" : "Resource type mapping",
      "description" : "One or more resource types mappings, where the left side of the mapping
 specifies the UUID of a resource type used by the input policies and the right side of the mapping
 specifies the UUID of a resource type used by the output policies. The two resource types should have
 the same resource patterns",
      "type" : "object",
      "additionalProperties" : {
        "type" : "string"
      }
    }
  },
  "required" : [ "from", "to" ]
}
```

query

Query the stored policies

Usage:

```
am> query Policies --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all. Fields that can be queried: [*]

read

Read policy

Usage:

```
am> read Policies --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Update an existing policy

Usage:

```
am> update Policies --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "$schema" : "http://json-schema.org/draft-04/schema#",
  "description" : "Json schema for the policy resource",
  "title" : "Policy Resource Schema",
  "type" : "object",
  "properties" : {
    "name" : {
      "title" : "Name",
      "description" : "String matching the name of the application",
```

```
      "type" : "string"
    },
    "active" : {
      "title" : "Active flag",
      "description" : "Boolean indicating whether OpenAM considers the policy active for evaluation
purposes, defaults to false",
      "type" : "boolean"
    },
    "description" : {
      "title" : "Description",
      "description" : "String describing the policy",
      "type" : "string"
    },
    "applicationName" : {
      "title" : "Application name",
      "description" : "String containing the application name, such as \"iPlanetAMWebAgentService\",
or \"mypolicyset\"",
      "type" : "string"
    },
    "actionValues" : {
      "title" : "Action values",
      "description" : "Set of string action names, each set to a boolean indicating whether the action
is allowed. Chosen from the available actions provided by the associated Managing Resource Types
resource type",
      "type" : "object",
      "additionalProperties" : {
        "type" : "boolean"
      }
    },
    "resources" : {
      "title" : "Resources",
      "description" : "List of the resource name pattern strings to which the policy applies. Must
conform to the pattern templates provided by the associated Managing Resource Types resource type",
      "type" : "array",
      "items" : {
        "type" : "string"
      }
    },
    "subject" : {
      "title" : "Subject",
      "description" : "Specifies the subject conditions to which the policy applies, where subjects
can be combined by using the built-in types \"AND\", \"OR\", and \"NOT\", and where subject
implementations are pluggable",
      "type" : "object"
    },
    "condition" : {
      "title" : "Condition",
      "description" : "Specifies environment conditions, where conditions can be combined by using the
built-in types \"AND\", \"OR\", and \"NOT\", and where condition implementations are pluggable",
      "type" : "object",
      "properties" : {
        "type" : {
          "type" : "string"
        },
        "conditions" : {
          "type" : "array",
          "title" : "Condition",
          "description" : "Specifies environment conditions, where conditions can be combined by using
the built-in types \"AND\", \"OR\", and \"NOT\", and where condition implementations are pluggable",
```

```
          "items" : {
            "type" : "object"
          }
        }
      }
    },
    "resourceTypeUuid" : {
      "title" : "Resource Type UUID",
      "description" : "The UUIDs of the resource type associated with the policy",
      "type" : "string"
    },
    "resourceAttributes" : {
      "title" : "Resource Attributes",
      "description" : "List of attributes to return with decisions. These attributes are known as
 response attributes",
      "type" : "array",
      "items" : {
        "type" : "object"
      }
    },
    "lastModifiedBy" : {
      "title" : "Last Modified By",
      "description" : "A string containing the universal identifier DN of the subject that most
 recently updated the policy",
      "type" : "string"
    },
    "lastModifiedDate" : {
      "title" : "Last Modified date",
      "description" : "An integer containing the last modified date and time, in number of seconds",
      "type" : "string"
    },
    "createdBy" : {
      "title" : "Created By",
      "description" : "A string containing the universal identifier DN of the subject that created the
 policy",
      "type" : "string"
    },
    "creationDate" : {
      "title" : "Creation Date",
      "description" : "An integer containing the creation date and time, in number of seconds",
      "type" : "string"
    }
  }
}
```

PolicyAgents

Realm Operations

Agents handler that is responsible for managing agents

Resource path: `/realm-config/agents/2.2_Agent`

Resource version: `1.0`

create

Usage:

```
am> create PolicyAgents --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "cdssoRootUrl" : {
      "title" : "Agent Key Value(s)",
      "description" : "Set the agent properties with a key/value pair. This property is used by AM to
 receive agent requests for credential assertions about users. Currently, only one property is valid
 and all other properties will be ignored. Use the following format: <br> agentRootURL=protocol://
hostname:port/ <br> The entry must be precise and agentRootURL is case sensitive.",
      "propertyOrder" : 22500,
      "items" : {
        "type" : "string"
      },
      "type" : "object",
      "exampleValue" : "",
      "properties" : {
        "inherited" : {
          "type" : "boolean",
          "required" : true
        },
        "value" : {
          "type" : "array",
          "required" : true
        }
      }
    },
    "userpassword" : {
      "title" : "Password",
      "description" : "",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "format" : "password",
      "exampleValue" : ""
    },
    "status" : {
      "title" : "Status",
      "description" : "Status of the agent configuration.",
      "propertyOrder" : 200,
      "type" : "object",
      "exampleValue" : "",
      "properties" : {
```

```
        "inherited" : {
          "type" : "boolean",
          "required" : true
        },
        "value" : {
          "type" : "string",
          "required" : true
        }
      }
    },
    "description" : {
      "title" : "Description",
      "description" : "",
      "propertyOrder" : 22400,
      "type" : "object",
      "exampleValue" : "",
      "properties" : {
        "inherited" : {
          "type" : "boolean",
          "required" : true
        },
        "value" : {
          "type" : "string",
          "required" : true
        }
      }
    }
  }
}
```

delete

Usage:

```
am> delete PolicyAgents --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action PolicyAgents --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action PolicyAgents --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action PolicyAgents --realm Realm --actionName nextdescendents
```

query

Querying the agents of a specific type

Usage:

```
am> query PolicyAgents --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read PolicyAgents --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update PolicyAgents --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "cdssoRootUrl" : {
      "title" : "Agent Key Value(s)",
      "description" : "Set the agent properties with a key/value pair. This property is used by AM to
 receive agent requests for credential assertions about users. Currently, only one property is valid
 and all other properties will be ignored. Use the following format: <br> agentRootURL=protocol://
hostname:port/ <br> The entry must be precise and agentRootURL is case sensitive.",
      "propertyOrder" : 22500,
      "items" : {
        "type" : "string"
      },
      "type" : "object",
      "exampleValue" : "",
      "properties" : {
        "inherited" : {
          "type" : "boolean",
          "required" : true
        },
        "value" : {
          "type" : "array",
          "required" : true
        }
      }
    },
    "userpassword" : {
      "title" : "Password",
      "description" : "",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "format" : "password",
      "exampleValue" : ""
    },
    "status" : {
      "title" : "Status",
      "description" : "Status of the agent configuration.",
      "propertyOrder" : 200,
      "type" : "object",
      "exampleValue" : "",
      "properties" : {
        "inherited" : {
          "type" : "boolean",
          "required" : true
        },
        "value" : {
          "type" : "string",
          "required" : true
        }
      }
    },
    "description" : {
      "title" : "Description",
      "description" : "",
```

```
      "propertyOrder" : 22400,
      "type" : "object",
      "exampleValue" : "",
      "properties" : {
        "inherited" : {
          "type" : "boolean",
          "required" : true
        },
        "value" : {
          "type" : "string",
          "required" : true
        }
      }
    }
  }
}
```

PolicyConfiguration

Realm Operations

Resource path: `/realm-config/services/policyconfiguration`

Resource version: `1.0`

create

Usage:

```
am> create PolicyConfiguration --realm Realm --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "maximumSearchResults" : {
      "title" : "Maximum Results Returned from Search",
      "description" : "Search limit for LDAP searches.",
      "propertyOrder" : 1400,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "usersSearchAttribute" : {
      "title" : "LDAP Users Search Attribute",
      "description" : "Naming attribute for user entries.",
```

```
      "propertyOrder" : 1300,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "searchTimeout" : {
      "title" : "Search Timeout",
      "description" : "Time after which OpenAM returns an error for an incomplete search, in
seconds.",
      "propertyOrder" : 1500,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "policyHeartbeatInterval" : {
      "title" : "Heartbeat Interval",
      "description" : "Specifies how often should OpenAM send a heartbeat request to the
directory.<br><br>Use this option in case a firewall/loadbalancer can close idle connections, since
the heartbeat requests will ensure that the connections won't become idle.",
      "propertyOrder" : 1840,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "usersBaseDn" : {
      "title" : "LDAP Users Base DN",
      "description" : "Base DN for LDAP Users subject searches.",
      "propertyOrder" : 500,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "userAliasEnabled" : {
      "title" : "User Alias",
      "description" : "If enabled, OpenAM can evaluate policy for remote users aliased to local
users.",
      "propertyOrder" : 2000,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "usersSearchScope" : {
      "title" : "LDAP Users Search Scope",
      "description" : "Search scope to find user entries.",
      "propertyOrder" : 1100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "policyHeartbeatTimeUnit" : {
      "title" : "Heartbeat Unit",
      "description" : "Defines the time unit corresponding to the Heartbeat Interval
setting.<br><br>Use this option in case a firewall/loadbalancer can close idle connections, since the
heartbeat requests will ensure that the connections won't become idle.",
      "propertyOrder" : 1850,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
```

```
   "connectionPoolMinimumSize" : {
     "title" : "LDAP Connection Pool Minimum Size",
     "description" : "Minimum number of connections in the pool.",
     "propertyOrder" : 1700,
     "required" : true,
     "type" : "integer",
     "exampleValue" : ""
   },
   "subjectsResultTTL" : {
     "title" : "Subjects Result Time to Live",
     "description" : "Maximum time that OpenAM caches a subject result for evaluating policy
requests, in minutes. A value of <code>0</code> prevents OpenAM from caching subject evaluations for
policy decisions.",
     "propertyOrder" : 1900,
     "required" : true,
     "type" : "integer",
     "exampleValue" : ""
   },
   "usersSearchFilter" : {
     "title" : "LDAP Users Search Filter",
     "description" : "Search filter to match user entries.",
     "propertyOrder" : 1000,
     "required" : true,
     "type" : "string",
     "exampleValue" : ""
   },
   "checkIfResourceTypeExists" : {
     "title" : "Check resources exist when Resource Server is updated",
     "description" : "Check all registered resources exist when updating Resource Server.
<p><p>Policy Set will check each registered Resource Types one by one against config datastore if
enabled. Consider disabling this option if you have large number of Resource Types registered to a
Policy Set.",
     "propertyOrder" : 2100,
     "required" : true,
     "type" : "boolean",
     "exampleValue" : ""
   },
   "bindDn" : {
     "title" : "LDAP Bind DN",
     "description" : "Bind DN to connect to the directory server for policy information.",
     "propertyOrder" : 700,
     "required" : true,
     "type" : "string",
     "exampleValue" : ""
   },
   "connectionPoolMaximumSize" : {
     "title" : "LDAP Connection Pool Maximum Size",
     "description" : "Maximum number of connections in the pool.",
     "propertyOrder" : 1800,
     "required" : true,
     "type" : "integer",
     "exampleValue" : ""
   },
   "realmSearchFilter" : {
     "title" : "LDAP Organization Search Filter",
     "description" : "Search filter to match organization entries.",
     "propertyOrder" : 900,
     "required" : true,
     "type" : "string",
```

```
      "exampleValue" : ""
    },
    "sslEnabled" : {
      "title" : "LDAP SSL/TLS",
      "description" : "If enabled, OpenAM connects securely to the directory server. This requires
 that you install the directory server certificate.",
      "propertyOrder" : 1600,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "ldapServer" : {
      "title" : "Primary LDAP Server",
      "description" : "Configuration directory server host:port that OpenAM searches for policy
 information.<p><p>Format: <code>local OpenAM server name | hostname:port</code><p><p>Multiple
 entries must be prefixed by local server name. Make sure to place the multiple entries on a single
 line and separate the hostname:port URLs with a space. <p><p>For example, openam.example.com|
opendj.example.com:1389 opendj.example.com:2389",
      "propertyOrder" : 400,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "bindPassword" : {
      "title" : "LDAP Bind Password",
      "description" : "Bind password to connect to the directory server for policy information.",
      "propertyOrder" : 800,
      "required" : true,
      "type" : "string",
      "format" : "password",
      "exampleValue" : ""
    }
  }
}
```

delete

Usage:

```
am> delete PolicyConfiguration --realm Realm
```

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action PolicyConfiguration --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action PolicyConfiguration --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action PolicyConfiguration --realm Realm --actionName nextdescendents
```

read

Usage:

```
am> read PolicyConfiguration --realm Realm
```

update

Usage:

```
am> update PolicyConfiguration --realm Realm --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "maximumSearchResults" : {
      "title" : "Maximum Results Returned from Search",
      "description" : "Search limit for LDAP searches.",
      "propertyOrder" : 1400,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "usersSearchAttribute" : {
      "title" : "LDAP Users Search Attribute",
      "description" : "Naming attribute for user entries.",
      "propertyOrder" : 1300,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
```

```
   "searchTimeout" : {
     "title" : "Search Timeout",
     "description" : "Time after which OpenAM returns an error for an incomplete search, in
seconds.",
     "propertyOrder" : 1500,
     "required" : true,
     "type" : "integer",
     "exampleValue" : ""
   },
   "policyHeartbeatInterval" : {
     "title" : "Heartbeat Interval",
     "description" : "Specifies how often should OpenAM send a heartbeat request to the
directory.<br><br>Use this option in case a firewall/loadbalancer can close idle connections, since
the heartbeat requests will ensure that the connections won't become idle.",
     "propertyOrder" : 1840,
     "required" : true,
     "type" : "integer",
     "exampleValue" : ""
   },
   "usersBaseDn" : {
     "title" : "LDAP Users Base DN",
     "description" : "Base DN for LDAP Users subject searches.",
     "propertyOrder" : 500,
     "required" : true,
     "type" : "string",
     "exampleValue" : ""
   },
   "userAliasEnabled" : {
     "title" : "User Alias",
     "description" : "If enabled, OpenAM can evaluate policy for remote users aliased to local
users.",
     "propertyOrder" : 2000,
     "required" : true,
     "type" : "boolean",
     "exampleValue" : ""
   },
   "usersSearchScope" : {
     "title" : "LDAP Users Search Scope",
     "description" : "Search scope to find user entries.",
     "propertyOrder" : 1100,
     "required" : true,
     "type" : "string",
     "exampleValue" : ""
   },
   "policyHeartbeatTimeUnit" : {
     "title" : "Heartbeat Unit",
     "description" : "Defines the time unit corresponding to the Heartbeat Interval
setting.<br><br>Use this option in case a firewall/loadbalancer can close idle connections, since the
heartbeat requests will ensure that the connections won't become idle.",
     "propertyOrder" : 1850,
     "required" : true,
     "type" : "string",
     "exampleValue" : ""
   },
   "connectionPoolMinimumSize" : {
     "title" : "LDAP Connection Pool Minimum Size",
     "description" : "Minimum number of connections in the pool.",
     "propertyOrder" : 1700,
     "required" : true,
```

```
      "type" : "integer",
      "exampleValue" : ""
    },
    "subjectsResultTTL" : {
      "title" : "Subjects Result Time to Live",
      "description" : "Maximum time that OpenAM caches a subject result for evaluating policy
requests, in minutes. A value of <code>0</code> prevents OpenAM from caching subject evaluations for
policy decisions.",
      "propertyOrder" : 1900,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "usersSearchFilter" : {
      "title" : "LDAP Users Search Filter",
      "description" : "Search filter to match user entries.",
      "propertyOrder" : 1000,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "checkIfResourceTypeExists" : {
      "title" : "Check resources exist when Resource Server is updated",
      "description" : "Check all registered resources exist when updating Resource Server.
<p><p>Policy Set will check each registered Resource Types one by one against config datastore if
enabled. Consider disabling this option if you have large number of Resource Types registered to a
Policy Set.",
      "propertyOrder" : 2100,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "bindDn" : {
      "title" : "LDAP Bind DN",
      "description" : "Bind DN to connect to the directory server for policy information.",
      "propertyOrder" : 700,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "connectionPoolMaximumSize" : {
      "title" : "LDAP Connection Pool Maximum Size",
      "description" : "Maximum number of connections in the pool.",
      "propertyOrder" : 1800,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "realmSearchFilter" : {
      "title" : "LDAP Organization Search Filter",
      "description" : "Search filter to match organization entries.",
      "propertyOrder" : 900,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "sslEnabled" : {
      "title" : "LDAP SSL/TLS",
```

```
      "description" : "If enabled, OpenAM connects securely to the directory server. This requires
 that you install the directory server certificate.",
      "propertyOrder" : 1600,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "ldapServer" : {
      "title" : "Primary LDAP Server",
      "description" : "Configuration directory server host:port that OpenAM searches for policy
 information.<p><p>Format: <code>local OpenAM server name | hostname:port</code><p><p>Multiple
 entries must be prefixed by local server name. Make sure to place the multiple entries on a single
 line and separate the hostname:port URLs with a space. <p><p>For example, openam.example.com|
opendj.example.com:1389 opendj.example.com:2389",
      "propertyOrder" : 400,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "bindPassword" : {
      "title" : "LDAP Bind Password",
      "description" : "Bind password to connect to the directory server for policy information.",
      "propertyOrder" : 800,
      "required" : true,
      "type" : "string",
      "format" : "password",
      "exampleValue" : ""
    }
  }
}
```

Global Operations

Resource path: `/global-config/services/policyconfiguration`

Resource version: `1.0`

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action PolicyConfiguration --global --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action PolicyConfiguration --global --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action PolicyConfiguration --global --actionName nextdescendents
```

read

Usage:

```
am> read PolicyConfiguration --global
```

update

Usage:

```
am> update PolicyConfiguration --global --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "continueEvaluationOnDeny" : {
      "title" : "Continue Evaluation on Deny Decision",
      "description" : "If no, then OpenAM stops evaluating policy as soon as it reaches a deny
 decision.",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "realmAliasReferrals" : {
      "title" : "Realm Alias Referrals",
      "description" : "If yes, then OpenAM allows creation of policies for HTTP and HTTPS resources
 whose FQDN matches the DNS alias for the realm even when no referral policy exists.",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "resourceComparators" : {
      "title" : "Resource Comparator",
      "description" : "OpenAM uses resource comparators to match resources specified in policy rules.
 When setting comparators on the command line, separate fields with <code>|</code> characters.",
```

```
      "propertyOrder" : 100,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "defaults" : {
      "properties" : {
        "sslEnabled" : {
          "title" : "LDAP SSL/TLS",
          "description" : "If enabled, OpenAM connects securely to the directory server. This requires
 that you install the directory server certificate.",
          "propertyOrder" : 1600,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "ldapServer" : {
          "title" : "Primary LDAP Server",
          "description" : "Configuration directory server host:port that OpenAM searches for policy
 information.<p><p>Format: <code>local OpenAM server name | hostname:port</code><p><p>Multiple
 entries must be prefixed by local server name. Make sure to place the multiple entries on a single
 line and separate the hostname:port URLs with a space. <p><p>For example, openam.example.com|
opendj.example.com:1389 opendj.example.com:2389",
          "propertyOrder" : 400,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "connectionPoolMaximumSize" : {
          "title" : "LDAP Connection Pool Maximum Size",
          "description" : "Maximum number of connections in the pool.",
          "propertyOrder" : 1800,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "usersBaseDn" : {
          "title" : "LDAP Users Base DN",
          "description" : "Base DN for LDAP Users subject searches.",
          "propertyOrder" : 500,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "bindDn" : {
          "title" : "LDAP Bind DN",
          "description" : "Bind DN to connect to the directory server for policy information.",
          "propertyOrder" : 700,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "usersSearchFilter" : {
```

```
          "title" : "LDAP Users Search Filter",
          "description" : "Search filter to match user entries.",
          "propertyOrder" : 1000,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "usersSearchScope" : {
          "title" : "LDAP Users Search Scope",
          "description" : "Search scope to find user entries.",
          "propertyOrder" : 1100,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "bindPassword" : {
          "title" : "LDAP Bind Password",
          "description" : "Bind password to connect to the directory server for policy information.",
          "propertyOrder" : 800,
          "required" : true,
          "type" : "string",
          "format" : "password",
          "exampleValue" : ""
        },
        "policyHeartbeatInterval" : {
          "title" : "Heartbeat Interval",
          "description" : "Specifies how often should OpenAM send a heartbeat request to the
directory.<br><br>Use this option in case a firewall/loadbalancer can close idle connections, since
the heartbeat requests will ensure that the connections won't become idle.",
          "propertyOrder" : 1840,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "searchTimeout" : {
          "title" : "Search Timeout",
          "description" : "Time after which OpenAM returns an error for an incomplete search, in
seconds.",
          "propertyOrder" : 1500,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "userAliasEnabled" : {
          "title" : "User Alias",
          "description" : "If enabled, OpenAM can evaluate policy for remote users aliased to local
users.",
          "propertyOrder" : 2000,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "policyHeartbeatTimeUnit" : {
          "title" : "Heartbeat Unit",
          "description" : "Defines the time unit corresponding to the Heartbeat Interval
setting.<br><br>Use this option in case a firewall/loadbalancer can close idle connections, since the
heartbeat requests will ensure that the connections won't become idle.",
          "propertyOrder" : 1850,
          "required" : true,
```

```
          "type" : "string",
          "exampleValue" : ""
        },
        "checkIfResourceTypeExists" : {
          "title" : "Check resources exist when Resource Server is updated",
          "description" : "Check all registered resources exist when updating Resource Server.
<p><p>Policy Set will check each registered Resource Types one by one against config datastore if
enabled. Consider disabling this option if you have large number of Resource Types registered to a
Policy Set.",
          "propertyOrder" : 2100,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "usersSearchAttribute" : {
          "title" : "LDAP Users Search Attribute",
          "description" : "Naming attribute for user entries.",
          "propertyOrder" : 1300,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "maximumSearchResults" : {
          "title" : "Maximum Results Returned from Search",
          "description" : "Search limit for LDAP searches.",
          "propertyOrder" : 1400,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "subjectsResultTTL" : {
          "title" : "Subjects Result Time to Live",
          "description" : "Maximum time that OpenAM caches a subject result for evaluating policy
requests, in minutes. A value of <code>0</code> prevents OpenAM from caching subject evaluations for
policy decisions.",
          "propertyOrder" : 1900,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "realmSearchFilter" : {
          "title" : "LDAP Organization Search Filter",
          "description" : "Search filter to match organization entries.",
          "propertyOrder" : 900,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "connectionPoolMinimumSize" : {
          "title" : "LDAP Connection Pool Minimum Size",
          "description" : "Minimum number of connections in the pool.",
          "propertyOrder" : 1700,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        }
      },
      "type" : "object",
      "title" : "Realm Defaults"
```

```
    }
  }
}
```

PollingWaitNode

Realm Operations

Resource path: `/realm-config/authentication/authenticationtrees/nodes/PollingWaitNode`

Resource version: `1.0`

create

Usage:

```
am> create PollingWaitNode --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "exitable" : {
      "title" : "Exitable",
      "description" : "Choose whether to display a link which allows the user to leave the node early.
 Creates a new outcome.",
      "propertyOrder" : 500,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "spamDetectionEnabled" : {
      "title" : "Enable Spam Detection",
      "description" : "Choose whether spam detection is enforced for this node. Creates a new
 outcome.",
      "propertyOrder" : 200,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "secondsToWait" : {
      "title" : "Seconds To Wait",
```

```
      "description" : "How many seconds to wait before proceeding to the next node in the tree.",
      "propertyOrder" : 100,
      "type" : "integer",
      "exampleValue" : ""
    },
    "exitMessage" : {
      "title" : "Exit Message",
      "description" : "Localisation overrides for the exit message. The whole string will be displayed
 as a link. This is a map of locale to message.",
      "propertyOrder" : 600,
      "patternProperties" : {
        ".*" : {
          "type" : "string"
        }
      },
      "type" : "object",
      "exampleValue" : ""
    },
    "waitingMessage" : {
      "title" : "Waiting Message",
      "description" : "Localisation overrides for the waiting message. May use {{time}} to get the
 number of seconds remaining. This is a map of locale to message.",
      "propertyOrder" : 400,
      "patternProperties" : {
        ".*" : {
          "type" : "string"
        }
      },
      "type" : "object",
      "exampleValue" : ""
    },
    "spamDetectionTolerance" : {
      "title" : "Spam Tolerance",
      "description" : "How many times a user may resubmit to this node before the authentication is
 failed.",
      "propertyOrder" : 300,
      "type" : "integer",
      "exampleValue" : ""
    }
  },
  "required" : [ "waitingMessage", "spamDetectionTolerance", "exitMessage", "spamDetectionEnabled",
 "exitable", "secondsToWait" ]
}
```

delete

Usage:

```
am> delete PollingWaitNode --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action PollingWaitNode --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action PollingWaitNode --realm Realm --actionName getCreatableTypes
```

listOutcomes

List the available outcomes for the node type.

Usage:

```
am> action PollingWaitNode --realm Realm --body body --actionName listOutcomes
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "title" : "Some configuration of the node. This does not need to be complete against the
 configuration schema."
}
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action PollingWaitNode --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query PollingWaitNode --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read PollingWaitNode --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update PollingWaitNode --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "exitable" : {
      "title" : "Exitable",
      "description" : "Choose whether to display a link which allows the user to leave the node early.
 Creates a new outcome.",
      "propertyOrder" : 500,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "spamDetectionEnabled" : {
      "title" : "Enable Spam Detection",
      "description" : "Choose whether spam detection is enforced for this node. Creates a new
 outcome.",
      "propertyOrder" : 200,
      "type" : "boolean",
      "exampleValue" : ""
    },
```

```
    "secondsToWait" : {
      "title" : "Seconds To Wait",
      "description" : "How many seconds to wait before proceeding to the next node in the tree.",
      "propertyOrder" : 100,
      "type" : "integer",
      "exampleValue" : ""
    },
    "exitMessage" : {
      "title" : "Exit Message",
      "description" : "Localisation overrides for the exit message. The whole string will be displayed
 as a link. This is a map of locale to message.",
      "propertyOrder" : 600,
      "patternProperties" : {
        ".*" : {
          "type" : "string"
        }
      },
      "type" : "object",
      "exampleValue" : ""
    },
    "waitingMessage" : {
      "title" : "Waiting Message",
      "description" : "Localisation overrides for the waiting message. May use {{time}} to get the
 number of seconds remaining. This is a map of locale to message.",
      "propertyOrder" : 400,
      "patternProperties" : {
        ".*" : {
          "type" : "string"
        }
      },
      "type" : "object",
      "exampleValue" : ""
    },
    "spamDetectionTolerance" : {
      "title" : "Spam Tolerance",
      "description" : "How many times a user may resubmit to this node before the authentication is
 failed.",
      "propertyOrder" : 300,
      "type" : "integer",
      "exampleValue" : ""
    }
  },
  "required" : [ "waitingMessage", "spamDetectionTolerance", "exitMessage", "spamDetectionEnabled",
 "exitable", "secondsToWait" ]
}
```

ProfileCompletenessDecision

Realm Operations

Resource path: `/realm-config/authentication/authenticationtrees/nodes/ProfileCompletenessDecisionNode`

Resource version: `1.0`

create

Usage:

```
am> create ProfileCompletenessDecision --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "identityAttribute" : {
      "title" : "Identity Attribute",
      "description" : "The attribute to query for the IDM object.",
      "propertyOrder" : 300,
      "type" : "string",
      "exampleValue" : ""
    },
    "threshold" : {
      "title" : "Profile Completeness Threshold",
      "description" : "Percentage of user-viewable and user-editable fields that must contain a value.
 Must be in the range of [0, 100].",
      "propertyOrder" : 100,
      "type" : "integer",
      "exampleValue" : ""
    }
  },
  "required" : [ "threshold", "identityAttribute" ]
}
```

delete

Usage:

```
am> delete ProfileCompletenessDecision --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action ProfileCompletenessDecision --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action ProfileCompletenessDecision --realm Realm --actionName getCreatableTypes
```

listOutcomes

List the available outcomes for the node type.

Usage:

```
am> action ProfileCompletenessDecision --realm Realm --body body --actionName listOutcomes
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "title" : "Some configuration of the node. This does not need to be complete against the
 configuration schema."
}
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action ProfileCompletenessDecision --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query ProfileCompletenessDecision --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read ProfileCompletenessDecision --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update ProfileCompletenessDecision --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "identityAttribute" : {
      "title" : "Identity Attribute",
      "description" : "The attribute to query for the IDM object.",
      "propertyOrder" : 300,
      "type" : "string",
      "exampleValue" : ""
    },
    "threshold" : {
      "title" : "Profile Completeness Threshold",
      "description" : "Percentage of user-viewable and user-editable fields that must contain a value.
 Must be in the range of [0, 100].",
      "propertyOrder" : 100,
      "type" : "integer",
      "exampleValue" : ""
    }
  },
  "required" : [ "threshold", "identityAttribute" ]
}
```

PrometheusReporter

Global Operations

Resource path: `/global-config/services/monitoring/prometheus`

Resource version: `1.0`

create

Usage:

```
am> create PrometheusReporter --global --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "authenticationType" : {
      "title" : "Authentication Type",
      "description" : "",
      "propertyOrder" : 150,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "password" : {
      "title" : "Password",
      "description" : "",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "string",
      "format" : "password",
      "exampleValue" : ""
    },
    "username" : {
      "title" : "Username",
      "description" : "",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
```

```
      "exampleValue" : ""
    },
    "enabled" : {
      "title" : "Enabled",
      "description" : "",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    }
  }
}
```

delete

Usage:

```
am> delete PrometheusReporter --global --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action PrometheusReporter --global --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action PrometheusReporter --global --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action PrometheusReporter --global --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query PrometheusReporter --global --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read PrometheusReporter --global --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update PrometheusReporter --global --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "authenticationType" : {
      "title" : "Authentication Type",
      "description" : "",
      "propertyOrder" : 150,
      "required" : true,
      "type" : "string",
```

```
      "exampleValue" : ""
    },
    "password" : {
      "title" : "Password",
      "description" : "",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "string",
      "format" : "password",
      "exampleValue" : ""
    },
    "username" : {
      "title" : "Username",
      "description" : "",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "enabled" : {
      "title" : "Enabled",
      "description" : "",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    }
  }
}
```

ProvisionDynamicAccount

Realm Operations

Resource path: `/realm-config/authentication/authenticationtrees/nodes/ProvisionDynamicAccountNode`

Resource version: `1.0`

create

Usage:

```
am> create ProvisionDynamicAccount --realm Realm --id id --body body
```

Parameters:

`--id`

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "accountProviderClass" : {
      "title" : "Account Provider Class",
      "description" : "",
      "propertyOrder" : 100,
      "type" : "string",
      "exampleValue" : ""
    }
  },
  "required" : [ "accountProviderClass" ]
}
```

delete

Usage:

```
am> delete ProvisionDynamicAccount --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action ProvisionDynamicAccount --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action ProvisionDynamicAccount --realm Realm --actionName getCreatableTypes
```

listOutcomes

List the available outcomes for the node type.

Usage:

```
am> action ProvisionDynamicAccount --realm Realm --body body --actionName listOutcomes
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "title" : "Some configuration of the node. This does not need to be complete against the
 configuration schema."
}
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action ProvisionDynamicAccount --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query ProvisionDynamicAccount --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read ProvisionDynamicAccount --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update ProvisionDynamicAccount --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "accountProviderClass" : {
      "title" : "Account Provider Class",
      "description" : "",
      "propertyOrder" : 100,
      "type" : "string",
      "exampleValue" : ""
    }
  },
  "required" : [ "accountProviderClass" ]
}
```

ProvisionIDMAccount

Realm Operations

Resource path: `/realm-config/authentication/authenticationtrees/nodes/ProvisionIdmAccountNode`

Resource version: `1.0`

create

Usage:

```
am> create ProvisionIDMAccount --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "accountProviderClass" : {
      "title" : "Account Provider Class",
      "description" : "",
      "propertyOrder" : 100,
      "type" : "string",
      "exampleValue" : ""
    }
  },
  "required" : [ "accountProviderClass" ]
}
```

delete

Usage:

```
am> delete ProvisionIDMAccount --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action ProvisionIDMAccount --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action ProvisionIDMAccount --realm Realm --actionName getCreatableTypes
```

listOutcomes

List the available outcomes for the node type.

Usage:

```
am> action ProvisionIDMAccount --realm Realm --body body --actionName listOutcomes
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "title" : "Some configuration of the node. This does not need to be complete against the
 configuration schema."
}
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action ProvisionIDMAccount --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query ProvisionIDMAccount --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read ProvisionIDMAccount --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update ProvisionIDMAccount --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "accountProviderClass" : {
      "title" : "Account Provider Class",
      "description" : "",
      "propertyOrder" : 100,
      "type" : "string",
      "exampleValue" : ""
    }
  },
  "required" : [ "accountProviderClass" ]
}
```

PushNotification

Realm Operations

Resource path: `/realm-config/services/pushNotification`

Resource version: `1.0`

create

Usage:

```
am> create PushNotification --realm Realm --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "delegateFactory" : {
      "title" : "Message Transport Delegate Factory",
      "description" : "The fully qualified class name of the factory
 responsible for creating the PushNotificationDelegate. The class must implement
 <code>org.forgerock.openam.services.push.PushNotificationDelegate</code>.",
      "propertyOrder" : 600,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "googleEndpoint" : {
      "title" : "SNS Endpoint for GCM",
      "description" : "The Simple Notification Service endpoint in Amazon Resource Name format, used
 to send push messages over Google Cloud Messaging (GCM).",
      "propertyOrder" : 400,
      "required" : true,
      "type" : "string",
      "exampleValue" : "arn:aws:sns:us-east-1:1234567890:app/GCM/production"
    },
    "mdConcurrency" : {
      "title" : "Response Cache Concurrency",
      "description" : "Level of concurrency to use when accessing the message dispatcher cache.
 Defaults to <code>16</code>, and must be greater than <code>0</code>. Choose a value to accommodate
 as many threads as will ever concurrently access the message dispatcher cache.",
      "propertyOrder" : 800,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "mdDuration" : {
      "title" : "Response Cache Duration",
      "description" : "The minimum lifetime to keep unanswered message records in the message
 dispatcher cache, in seconds. To keep unanswered message records indefinitely, set this property to
 <code>0</code>.Should be tuned so that it is applicable to the use case of this service. For example,
 the ForgeRock Authenticator (Push) authentication module has a default timeout of 120 seconds.",
      "propertyOrder" : 700,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "accessKey" : {
      "title" : "SNS Access Key ID",
      "description" : "Amazon Simple Notification Service Access Key ID. For more information, see
 <a href=\"https://aws.amazon.com/developers/access-keys/\">https://aws.amazon.com/developers/access-
keys/</a>.",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "exampleValue" : "AKIAIOSFODNN7EXAMPLE"
    },
    "appleEndpoint" : {
      "title" : "SNS Endpoint for APNS",
```

```
      "description" : "The Simple Notification Service endpoint in Amazon Resource Name format, used
 to send push messages to the Apple Push Notification Service (APNS).",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "string",
      "exampleValue" : "arn:aws:sns:us-east-1:1234567890:app/APNS/production"
    },
    "mdCacheSize" : {
      "title" : "Response Cache Size",
      "description" : "Maximum size of the message dispatcher cache, in number of records. If set
 to <code>0</code> the cache can grow indefinitely. If the number of records that need to be stored
 exceeds this maximum, then older items in the cache will be removed to make space.",
      "propertyOrder" : 900,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "secret" : {
      "title" : "SNS Access Key Secret",
      "description" : "Amazon Simple Notification Service Access Key Secret. For more information, see
 <a href=\"https://aws.amazon.com/developers/access-keys/\">https://aws.amazon.com/developers/access-
keys/</a>.",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
      "format" : "password",
      "exampleValue" : ""
    },
    "region" : {
      "title" : "SNS Client Region",
      "description" : "Region of your registered Amazon Simple Notification Service client. For
 more information, see <a href=\"https://docs.aws.amazon.com/general/latest/gr/rande.html\">https://
docs.aws.amazon.com/general/latest/gr/rande.html</a>.",
      "propertyOrder" : 500,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
```

delete

Usage:

```
am> delete PushNotification --realm Realm
```

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action PushNotification --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action PushNotification --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action PushNotification --realm Realm --actionName nextdescendents
```

read

Usage:

```
am> read PushNotification --realm Realm
```

update

Usage:

```
am> update PushNotification --realm Realm --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "delegateFactory" : {
      "title" : "Message Transport Delegate Factory",
      "description" : "The fully qualified class name of the factory
 responsible for creating the PushNotificationDelegate. The class must implement
 <code>org.forgerock.openam.services.push.PushNotificationDelegate</code>.",
      "propertyOrder" : 600,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "googleEndpoint" : {
      "title" : "SNS Endpoint for GCM",
      "description" : "The Simple Notification Service endpoint in Amazon Resource Name format, used
 to send push messages over Google Cloud Messaging (GCM).",
      "propertyOrder" : 400,
      "required" : true,
```

```
      "type" : "string",
      "exampleValue" : "arn:aws:sns:us-east-1:1234567890:app/GCM/production"
    },
    "mdConcurrency" : {
      "title" : "Response Cache Concurrency",
      "description" : "Level of concurrency to use when accessing the message dispatcher cache.
 Defaults to <code>16</code>, and must be greater than <code>0</code>. Choose a value to accommodate
 as many threads as will ever concurrently access the message dispatcher cache.",
      "propertyOrder" : 800,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "mdDuration" : {
      "title" : "Response Cache Duration",
      "description" : "The minimum lifetime to keep unanswered message records in the message
 dispatcher cache, in seconds. To keep unanswered message records indefinitely, set this property to
 <code>0</code>.Should be tuned so that it is applicable to the use case of this service. For example,
 the ForgeRock Authenticator (Push) authentication module has a default timeout of 120 seconds.",
      "propertyOrder" : 700,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "accessKey" : {
      "title" : "SNS Access Key ID",
      "description" : "Amazon Simple Notification Service Access Key ID. For more information, see
 <a href=\"https://aws.amazon.com/developers/access-keys/\">https://aws.amazon.com/developers/access-
keys/</a>.",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "exampleValue" : "AKIAIOSFODNN7EXAMPLE"
    },
    "appleEndpoint" : {
      "title" : "SNS Endpoint for APNS",
      "description" : "The Simple Notification Service endpoint in Amazon Resource Name format, used
 to send push messages to the Apple Push Notification Service (APNS).",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "string",
      "exampleValue" : "arn:aws:sns:us-east-1:1234567890:app/APNS/production"
    },
    "mdCacheSize" : {
      "title" : "Response Cache Size",
      "description" : "Maximum size of the message dispatcher cache, in number of records. If set
 to <code>0</code> the cache can grow indefinitely. If the number of records that need to be stored
 exceeds this maximum, then older items in the cache will be removed to make space.",
      "propertyOrder" : 900,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "secret" : {
      "title" : "SNS Access Key Secret",
      "description" : "Amazon Simple Notification Service Access Key Secret. For more information, see
 <a href=\"https://aws.amazon.com/developers/access-keys/\">https://aws.amazon.com/developers/access-
keys/</a>.",
      "propertyOrder" : 200,
```

```
      "required" : true,
      "type" : "string",
      "format" : "password",
      "exampleValue" : ""
    },
    "region" : {
      "title" : "SNS Client Region",
      "description" : "Region of your registered Amazon Simple Notification Service client. For
 more information, see <a href=\"https://docs.aws.amazon.com/general/latest/gr/rande.html\">https://
docs.aws.amazon.com/general/latest/gr/rande.html</a>.",
      "propertyOrder" : 500,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
```

Global Operations

Resource path: `/global-config/services/pushNotification`

Resource version: `1.0`

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action PushNotification --global --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action PushNotification --global --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action PushNotification --global --actionName nextdescendents
```

read

Usage:

```
am> read PushNotification --global
```

update

Usage:

```
am> update PushNotification --global --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "defaults" : {
      "properties" : {
        "mdCacheSize" : {
          "title" : "Response Cache Size",
          "description" : "Maximum size of the message dispatcher cache, in number of records. If set
 to <code>0</code> the cache can grow indefinitely. If the number of records that need to be stored
 exceeds this maximum, then older items in the cache will be removed to make space.",
          "propertyOrder" : 900,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "accessKey" : {
          "title" : "SNS Access Key ID",
          "description" : "Amazon Simple Notification Service Access Key ID. For more information, see
 <a href=\"https://aws.amazon.com/developers/access-keys/\">https://aws.amazon.com/developers/access-
keys/</a>.",
          "propertyOrder" : 100,
          "required" : true,
          "type" : "string",
          "exampleValue" : "AKIAIOSFODNN7EXAMPLE"
        },
        "appleEndpoint" : {
          "title" : "SNS Endpoint for APNS",
          "description" : "The Simple Notification Service endpoint in Amazon Resource Name format,
 used to send push messages to the Apple Push Notification Service (APNS).",
          "propertyOrder" : 300,
          "required" : true,
          "type" : "string",
          "exampleValue" : "arn:aws:sns:us-east-1:1234567890:app/APNS/production"
        },
        "secret" : {
          "title" : "SNS Access Key Secret",
          "description" : "Amazon Simple Notification Service Access Key Secret. For more information,
 see <a href=\"https://aws.amazon.com/developers/access-keys/\">https://aws.amazon.com/developers/
access-keys/</a>.",
          "propertyOrder" : 200,
          "required" : true,
```

```
          "type" : "string",
          "format" : "password",
          "exampleValue" : ""
        },
        "googleEndpoint" : {
          "title" : "SNS Endpoint for GCM",
          "description" : "The Simple Notification Service endpoint in Amazon Resource Name format,
 used to send push messages over Google Cloud Messaging (GCM).",
          "propertyOrder" : 400,
          "required" : true,
          "type" : "string",
          "exampleValue" : "arn:aws:sns:us-east-1:1234567890:app/GCM/production"
        },
        "mdConcurrency" : {
          "title" : "Response Cache Concurrency",
          "description" : "Level of concurrency to use when accessing the message dispatcher cache.
 Defaults to <code>16</code>, and must be greater than <code>0</code>. Choose a value to accommodate
 as many threads as will ever concurrently access the message dispatcher cache.",
          "propertyOrder" : 800,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "mdDuration" : {
          "title" : "Response Cache Duration",
          "description" : "The minimum lifetime to keep unanswered message records in the message
 dispatcher cache, in seconds. To keep unanswered message records indefinitely, set this property to
 <code>0</code>.Should be tuned so that it is applicable to the use case of this service. For example,
 the ForgeRock Authenticator (Push) authentication module has a default timeout of 120 seconds.",
          "propertyOrder" : 700,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "region" : {
          "title" : "SNS Client Region",
          "description" : "Region of your registered Amazon Simple Notification Service client. For
 more information, see <a href=\"https://docs.aws.amazon.com/general/latest/gr/rande.html\">https://
docs.aws.amazon.com/general/latest/gr/rande.html</a>.",
          "propertyOrder" : 500,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "delegateFactory" : {
          "title" : "Message Transport Delegate Factory",
          "description" : "The fully qualified class name of the factory
 responsible for creating the PushNotificationDelegate. The class must implement
 <code>org.forgerock.openam.services.push.PushNotificationDelegate</code>.",
          "propertyOrder" : 600,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      },
      "type" : "object",
      "title" : "Realm Defaults"
    }
  }
```

```
}
```

PushNotificationResponse

Realm Operations

Push Authentication depends on the secure verification of information sent from the server to the client, and from the client to the server. This allows the server to verify that the notification was received by the original device, and for the device to verify that only the server sent out the original request. This endpoint provides the place for the device to return responses to the server to requests received either by QR code or by push notification.

Resource path: `/push/sns/message`

Resource version: `1.0`

authenticate

Message sent from device to server in response to a request for authentication sent to the device via Push notification. This message is generally sent from the ForgeRock Authenticator app.

Usage:

```
am> action PushNotificationResponse --realm Realm --body body --actionName authenticate
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "messageId" : {
      "type" : "string",
      "title" : "Message ID",
      "description" : "Unique message identifier"
    },
    "jwt" : {
      "type" : "string",
      "title" : "JWT",
      "description" : "Signed JWT containing claims:\n* `response`: Response to challenge (Base64
 encoding of the HmacSHA256 hashing of the decoded shared secret and the decoded challenge)\n* `deny`:
 Indication that this auth attempt should be shut down (boolean)"
    }
  },
  "required" : [ "messageId", "jwt" ]
}
```

register

Message sent from device to server in response to a registration message received on the device via a QR code. This message is generally sent from the ForgeRock Authenticator app.

Usage:

```
am> action PushNotificationResponse --realm Realm --body body --actionName register
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "messageId" : {
      "type" : "string",
      "title" : "Message ID",
      "description" : "Unique message identifier"
    },
    "jwt" : {
      "type" : "string",
      "title" : "JWT",
      "description" : "Signed JWT containing claims:\n* `response`: Response to challenge (Base64
 encoding of the HmacSHA256 hashing of the decoded shared secret and the decoded challenge)\n*
 `mechanismUid`: The device-specific identifier for the just-registered mechanism (string)\n*
 `deviceId`: The registration token used by GCM or APNS (string)\n* `deviceType`: `android` or `ios`
 (string)\n* `communicationType`: `gcm` or `apns` (string)"
    }
  },
  "required" : [ "messageId", "jwt" ]
}
```

PushResultVerifierNode

Realm Operations

Resource path: `/realm-config/authentication/authenticationtrees/nodes/PushResultVerifierNode`

Resource version: `1.0`

create

Usage:

```
am> create PushResultVerifierNode --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "required" : [ ]
}
```

delete

Usage:

```
am> delete PushResultVerifierNode --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action PushResultVerifierNode --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action PushResultVerifierNode --realm Realm --actionName getCreatableTypes
```

listOutcomes

List the available outcomes for the node type.

Usage:

```
am> action PushResultVerifierNode --realm Realm --body body --actionName listOutcomes
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "title" : "Some configuration of the node. This does not need to be complete against the
 configuration schema."
}
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action PushResultVerifierNode --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query PushResultVerifierNode --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read PushResultVerifierNode --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update PushResultVerifierNode --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "required" : [ ]
}
```

PushSender

Realm Operations

Resource path: `/realm-config/authentication/authenticationtrees/nodes/PushAuthenticationSenderNode`

Resource version: `1.0`

create

Usage:

```
am> create PushSender --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "userMessage" : {
      "title" : "User Message",
      "description" : "The message to send to the user. {{user}} and {{issuer}} may be used as
 wildcards.",
      "propertyOrder" : 200,
```

```
      "patternProperties" : {
        ".*" : {
          "type" : "string"
        }
      },
      "type" : "object",
      "exampleValue" : ""
    },
    "mandatory" : {
      "title" : "Remove 'skip' option",
      "description" : "If checked, users will no longer be able to skip the module, and must interact
 with it.",
      "propertyOrder" : 300,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "messageTimeout" : {
      "title" : "Message Timeout",
      "description" : "The duration (in ms) that the message will time out after.",
      "propertyOrder" : 100,
      "type" : "integer",
      "exampleValue" : ""
    }
  },
  "required" : [ "mandatory", "messageTimeout", "userMessage" ]
}
```

delete

Usage:

```
am> delete PushSender --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action PushSender --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action PushSender --realm Realm --actionName getCreatableTypes
```

listOutcomes

List the available outcomes for the node type.

Usage:

```
am> action PushSender --realm Realm --body body --actionName listOutcomes
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "title" : "Some configuration of the node. This does not need to be complete against the
 configuration schema."
}
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action PushSender --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query PushSender --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read PushSender --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update PushSender --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "userMessage" : {
      "title" : "User Message",
      "description" : "The message to send to the user. {{user}} and {{issuer}} may be used as
 wildcards.",
      "propertyOrder" : 200,
      "patternProperties" : {
        ".*" : {
          "type" : "string"
        }
      },
      "type" : "object",
      "exampleValue" : ""
    },
    "mandatory" : {
      "title" : "Remove 'skip' option",
      "description" : "If checked, users will no longer be able to skip the module, and must interact
 with it.",
      "propertyOrder" : 300,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "messageTimeout" : {
      "title" : "Message Timeout",
      "description" : "The duration (in ms) that the message will time out after.",
      "propertyOrder" : 100,
      "type" : "integer",
      "exampleValue" : ""
    }
  },
  "required" : [ "mandatory", "messageTimeout", "userMessage" ]
}
```

PushUserDevices

Realm Operations

The Push devices service is responsible for exposing functions to change the collection of Push authentication devices. The supported methods are action, delete, query

Resource path: `/users/{user}/devices/2fa/push`

Resource version: `1.0`

check

Checks if the user's Authenticator Push module is 'skippable' and returns the result as a boolean

Usage:

```
am> action PushUserDevices --realm Realm --body body --user user --actionName check
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "$schema" : "http://json-schema.org/draft-04/schema#",
  "description" : "Push user device check action request schema",
  "type" : "object",
  "title" : "Push user device check action request schema"
}
```

--user

The Push devices service is responsible for exposing functions to change the collection of Push authentication devices. The supported methods are action, delete, query

delete

Delete Push user device

Usage:

```
am> delete PushUserDevices --realm Realm --id id --user user
```

Parameters:

--id

The unique identifier for the resource.

--user

The Push devices service is responsible for exposing functions to change the collection of Push authentication devices. The supported methods are action, delete, query

query

Query the user's device profile

Usage:

```
am> query PushUserDevices --realm Realm --filter filter --user user
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all. Fields that can be queried: [*]

--user

The Push devices service is responsible for exposing functions to change the collection of Push authentication devices. The supported methods are action, delete, query

reset

Sets the user's 'skippable' selection of Authenticator Push module to default (NOT_SET) and deletes their profile's attribute

Usage:

```
am> action PushUserDevices --realm Realm --body body --user user --actionName reset
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "$schema" : "http://json-schema.org/draft-04/schema#",
  "description" : "Push user device reset action request schema",
  "type" : "object",
  "title" : "Push user device reset action request schema"
}
```

--user

The Push devices service is responsible for exposing functions to change the collection of Push authentication devices. The supported methods are action, delete, query

skip

Sets the user's ability to skip an Authenticator Push module

Usage:

```
am> action PushUserDevices --realm Realm --body body --user user --actionName skip
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "description" : "Push user device skip action request schema",
  "type" : "object",
  "title" : "Push user device skip action request schema",
  "properties" : {
    "value" : {
      "type" : "boolean",
      "title" : "Skip push module response value",
      "description" : "True if the push device is set to skipped"
    }
  },
  "required" : [ "value" ]
}
```

--user

The Push devices service is responsible for exposing functions to change the collection of Push authentication devices. The supported methods are action, delete, query

QueryFilterDecision

Realm Operations

Resource path: `/realm-config/authentication/authenticationtrees/nodes/QueryFilterDecisionNode`

Resource version: `1.0`

create

Usage:

```
am> create QueryFilterDecision --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "identityAttribute" : {
      "title" : "Identity Attribute",
      "description" : "The attribute used to retrieve the object to be tested against the query
 filter.",
      "propertyOrder" : 200,
      "type" : "string",
      "exampleValue" : ""
    },
    "queryFilter" : {
      "title" : "Query Filter",
      "description" : "A query filter tested against an object.",
      "propertyOrder" : 100,
      "type" : "string",
      "exampleValue" : ""
    }
  },
  "required" : [ "queryFilter", "identityAttribute" ]
}
```

delete

Usage:

```
am> delete QueryFilterDecision --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action QueryFilterDecision --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action QueryFilterDecision --realm Realm --actionName getCreatableTypes
```

listOutcomes

List the available outcomes for the node type.

Usage:

```
am> action QueryFilterDecision --realm Realm --body body --actionName listOutcomes
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "title" : "Some configuration of the node. This does not need to be complete against the
 configuration schema."
}
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action QueryFilterDecision --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query QueryFilterDecision --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read QueryFilterDecision --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update QueryFilterDecision --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "identityAttribute" : {
      "title" : "Identity Attribute",
      "description" : "The attribute used to retrieve the object to be tested against the query
 filter.",
      "propertyOrder" : 200,
      "type" : "string",
      "exampleValue" : ""
    },
    "queryFilter" : {
      "title" : "Query Filter",
      "description" : "A query filter tested against an object.",
      "propertyOrder" : 100,
      "type" : "string",
      "exampleValue" : ""
    }
  },
  "required" : [ "queryFilter", "identityAttribute" ]
}
```

RESTSecurityTokenServices

Realm Operations

The REST STS endpoint is responsible for storing the configuration of instances of REST Security Token Services (STS). Available operations are create, read, update, delete, query, schema and template.

Resource path: `/realm-config/services/sts/rest-sts`

Resource version: `1.0`

create

Usage:

```
am> create RESTSecurityTokenServices --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "restStsSaml2" : {
      "type" : "object",
      "title" : "SAML2 Token",
      "propertyOrder" : 2,
      "properties" : {
        "saml2-custom-attribute-mapper-class-name" : {
          "title" : "Custom Attribute Mapper Class Name",
          "description" : "If the class implementing attribute mapping for attributes
 contained in the issued SAML2 assertion needs to be customized, implement the
 <code>org.forgerock.openam.sts.tokengeneration.saml2.statements.AttributeMapper</code> interface, and
 specify the class name of the implementation here.",
          "propertyOrder" : 2100,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "saml2-keystore-filename" : {
          "title" : "KeystorePath",
          "description" : "Path to keystore<br><br>Provide either the full filesystem path to a
 filesystem resident keystore, or a classpath-relative path to a keystore bundled in the OpenAM .war
 file. This keystore contains the IdP public/private keys and SP public key for signed and/or
 encrypted assertions. If assertions are neither signed nor encrypted, these values need not be
 specified.",
          "propertyOrder" : 2900,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "saml2-signature-key-password" : {
          "title" : "Signature Key Password",
          "description" : "",
          "propertyOrder" : 3400,
          "required" : false,
```

```
          "type" : "string",
          "format" : "password",
          "exampleValue" : ""
        },
        "saml2-custom-authentication-statements-provider-class-name" : {
          "title" : "Custom AuthenticationStatements Class Name",
          "description" : "If the AuthenticationStatements of
 the issued SAML2 assertion need to be customized, implement the
 <code>org.forgerock.openam.sts.tokengeneration.saml2.statements.AuthenticationStatementsProvider</
code> interface, and specify the class name of the implementation here.",
          "propertyOrder" : 1800,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "saml2-encrypt-nameid" : {
          "title" : "Encrypt NameID",
          "description" : "Check this box if the assertion NameID should be encrypted. If this box is
 checked, the Encrypt Assertion box cannot be checked.",
          "propertyOrder" : 2700,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "saml2-sp-entity-id" : {
          "title" : "Service Provider Entity Id",
          "description" : "Values will be used to populate the Audiences of the AudienceRestriction
 element of the Conditions element. This value is required when issuing Bearer assertions. See section
 4.1.4.2 of Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0 for details.",
          "propertyOrder" : 1200,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "saml2-custom-attribute-statements-provider-class-name" : {
          "title" : "Custom AttributeStatements Class Name",
          "description" : "If the AttributeStatements of the
 issued SAML2 assertion need to be customized, implement the
 <code>org.forgerock.openam.sts.tokengeneration.saml2.statements.AttributeStatementsProvider</code>
 interface, and specify the class name of the implementation here.",
          "propertyOrder" : 1900,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "saml2-attribute-map" : {
          "title" : "Attribute Mappings",
          "description" : "Contains the mapping of assertion attribute names (Map
 keys) to local OpenAM attributes (Map values) in configured data stores. Format:
 <code>assertion_attr_name=ldap_attr_name</code><br><br>The DefaultAttributeMapper looks at
 profile attributes in configured data stores, or in Session properties. The keys will define
 the name of the attributes included in the Assertion Attribute statements, and the data
 pulled from the subject's directory entry or session state corresponding to the map value
 will define the value corresponding to this attribute name. The keys can have the format
 <code>[NameFomatURI|]SAML ATTRIBUTE NAME</code>. If the attribute value is enclosed in quotes,
 that quoted value will be included in the attribute without mapping. Binary attributes should be
 followed by ';binary'. <br>Examples: <ul><li>EmailAddress=mail</li><li>Address=postaladdress</
li><li>urn:oasis:names:tc:SAML:2.0:attrname-format:uri|urn:mace:dir:attribute-def:cn=cn</
li><li>partnerID=\"staticPartnerIDValue\"</li><li>urn:oasis:names:tc:SAML:2.0:attrname-format:uri|
```

```
nameID=\"staticNameIDValue\"</li><li>photo=photo;binary</li><li>urn:oasis:names:tc:SAML:2.0:attrname-
format:uri|photo=photo;binary</li></ul>",
          "propertyOrder" : 2300,
          "required" : false,
          "patternProperties" : {
            ".*" : {
              "type" : "string"
            }
          },
          "type" : "object",
          "exampleValue" : ""
        },
        "saml2-token-lifetime-seconds" : {
          "title" : "Token Lifetime (Seconds)",
          "description" : "Set to over-ride the default of 600 (10 minutes).",
          "propertyOrder" : 1500,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "saml2-keystore-password" : {
          "title" : "Keystore Password",
          "description" : "",
          "propertyOrder" : 3000,
          "required" : false,
          "type" : "string",
          "format" : "password",
          "exampleValue" : ""
        },
        "saml2-encryption-key-alias" : {
          "title" : "Encryption Key Alias",
          "description" : "This alias corresponds to the SP's x509 Certificate identified by the SP
 Entity ID for this rest-sts instance. Not necessary unless assertions are to be encrypted.",
          "propertyOrder" : 3200,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "saml2-name-id-format" : {
          "title" : "NameIdFormat",
          "description" : "The default value is <code>urn:oasis:names:tc:SAML:1.1:nameid-
format:unspecified</code><br><br>See section 8.3 of <a href=\"http://docs.oasis-open.org/security/
saml/v2.0/saml-core-2.0-os.pdf\" target=\"_blank\">Assertions and Protocols for the OASIS Security
 Assertion Markup Language (SAML) V2.0</a> for details on possible values.",
          "propertyOrder" : 1400,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "saml2-encryption-algorithm-strength" : {
          "title" : "Encryption Algorithm Strength",
          "description" : "",
          "propertyOrder" : 2850,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "saml2-signature-key-alias" : {
          "title" : "Signature Key Alias",
```

```
          "description" : "Corresponds to the private key of the IdP. Will be used to sign assertions.
 Value can remain unspecified unless assertions are signed.",
          "propertyOrder" : 3300,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "saml2-encrypt-assertion" : {
          "title" : "Encrypt Assertion",
          "description" : "Check this box if the entire assertion should be encrypted. If this box is
 checked, the Encrypt NameID and Encrypt Attributes boxes cannot be checked.",
          "propertyOrder" : 2500,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "issuer-name" : {
          "title" : "The SAML2 Issuer Id",
          "description" : "The name of the issuer<br><br>This name will appear in some issued tokens -
 e.g. in the <code>saml:Issuer</code> of issued SAML2 assertions.",
          "propertyOrder" : 1100,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "saml2-sign-assertion" : {
          "title" : "Sign Assertion",
          "description" : "",
          "propertyOrder" : 2400,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "saml2-custom-conditions-provider-class-name" : {
          "title" : "Custom Conditions Provider Class Name",
          "description" : "If the Conditions of the issued SAML2 assertion need to be customized,
 implement the <code>org.forgerock.openam.sts.tokengeneration.saml2.statements.ConditionsProvider</
code> interface, and specify the class name of the implementation here.",
          "propertyOrder" : 1600,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "saml2-encrypt-attributes" : {
          "title" : "Encrypt Attributes",
          "description" : "Check this box if the assertion Attributes should be encrypted. If this box
 is checked, the Encrypt Assertion box cannot be checked.",
          "propertyOrder" : 2600,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "saml2-custom-subject-provider-class-name" : {
          "title" : "Customs Subject Provider Class Name",
          "description" : "If the Subject of the issued SAML2 assertion needs to be customized,
 implement the <code>org.forgerock.openam.sts.tokengeneration.saml2.statements.SubjectProvider</code>
 interface, and specify the class name of the implementation here.",
          "propertyOrder" : 1700,
          "required" : false,
```

```
          "type" : "string",
          "exampleValue" : ""
        },
        "saml2-custom-authz-decision-statements-provider-class-name" : {
          "title" : "Custom Authorization Decision Statements Class Name",
          "description" : "If the AuthorizationDecisionStatements
 of the issued SAML2 assertion need to be customized, implement the
 <code>org.forgerock.openam.sts.tokengeneration.saml2.statements.AuthzDecisionStatementsProvider</
code> interface, and specify the class name of the implementation here.",
          "propertyOrder" : 2000,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "saml2-key-transport-algorithm" : {
          "title" : "Key Transport Algorithm",
          "description" : "This setting controls the encryption algorithm used to encrypt the
 symmetric encryption key when SAML2 token encryption is enabled. Valid values include: <pre>http://
www.w3.org/2001/04/xmlenc#rsa-1_5</pre>, <pre>http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p</pre>,
 and <pre>http://www.w3.org/2009/xmlenc11#rsa-oaep</pre>",
          "propertyOrder" : 2860,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "saml2-custom-authn-context-mapper-class-name" : {
          "title" : "Custom Authentication Context Class Name",
          "description" : "If the AuthnContext mapping implemented by the
 <code>org.forgerock.openam.sts.rest.token.provider.saml.DefaultSaml2JsonTokenAuthnContextMapper</
code> class needs to be customized, implement the
 <code>org.forgerock.openam.sts.rest.token.provider.saml.Saml2JsonTokenAuthnContextMapper</code>
 interface, and specify the name of the implementation here.",
          "propertyOrder" : 2200,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "saml2-encryption-algorithm" : {
          "title" : "Encryption Algorithm",
          "description" : "Algorithm used to encrypt generated assertions.",
          "propertyOrder" : 2800,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "saml2-sp-acs-url" : {
          "title" : "Service Provider Assertion Consumer Service Url",
          "description" : "When issuing bearer assertions, the recipient attribute of the
 SubjectConfirmation element must be set to the Service Provider Assertion Consumer Service Url. See
 section 4.1.4.2 of Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0 for details.
 Value required when issuing Bearer assertions.",
          "propertyOrder" : 1300,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "restStsOidc" : {
```

```
      "type" : "object",
      "title" : "OpenID Connect Token",
      "propertyOrder" : 3,
      "properties" : {
        "oidc-authorized-party" : {
          "title" : "Authorized Party",
          "description" : "",
          "propertyOrder" : 4700,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "oidc-signature-algorithm" : {
          "title" : "Token Signature Algorithm",
          "description" : "Algorithm used to sign issued OIDC tokens",
          "propertyOrder" : 3600,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "oidc-issuer" : {
          "title" : "The OpenID Connect Token Provider Issuer Id",
          "description" : "",
          "propertyOrder" : 3450,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "oidc-custom-authn-method-references-mapper-class" : {
          "title" : "Custom Authn Methods References Mapper Class",
          "description" : "If issued OIDC tokens are to contain amr claims, implement the
 <code>org.forgerock.openam.sts.rest.token.provider.oidc.OpenIdConnectTokenAuthMethodReferencesMapper</
code> interface, and specify the class name of the implementation here.",
          "propertyOrder" : 5100,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "oidc-custom-claim-mapper-class" : {
          "title" : "Custom Claim Mapper Class",
          "description" : "If the class implementing attribute mapping for attributes
 contained in issued OpenID Connect tokens needs to be customized, implement the
 <code>org.forgerock.openam.sts.tokengeneration.oidc.OpenIdConnectTokenClaimMapper</code> interface,
 and specify the class name of the implementation here.",
          "propertyOrder" : 4900,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "oidc-keystore-password" : {
          "title" : "KeyStore Password",
          "description" : "",
          "propertyOrder" : 3900,
          "required" : true,
          "type" : "string",
          "format" : "password",
          "exampleValue" : ""
        },
        "oidc-client-secret" : {
```

```
          "title" : "Client Secret",
          "description" : "For HMAC-signed tokens, the client secret used as the HMAC key.<br><br>For
 HMAC-signed tokens, the KeyStore location, password, signature key alias and password configurations
 are not required.",
          "propertyOrder" : 4400,
          "required" : true,
          "type" : "string",
          "format" : "password",
          "exampleValue" : ""
        },
        "oidc-public-key-reference-type" : {
          "title" : "Public Key Reference Type",
          "description" : "For tokens signed with RSA, how should corresponding public key be
 referenced in the issued jwt",
          "propertyOrder" : 3700,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "oidc-audience" : {
          "title" : "Issued Tokens Audience",
          "description" : "Contents will be set in the aud claim",
          "propertyOrder" : 4600,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "oidc-keystore-location" : {
          "title" : "KeyStore Location",
          "description" : "For RSA-signed tokens, the filesystem or classpath location of the KeyStore
 containing signing key entry<br><br>For RSA-signed tokens, the KeyStore location, password, signing-
key alias, and signing key password must be specified. The client secret is not required for RSA-
signed tokens.",
          "propertyOrder" : 3800,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "oidc-claim-map" : {
          "title" : "Claim Map",
          "description" : "Contains the mapping of OIDC token claim names (Map keys) to local
 OpenAM attributes (Map values) in configured data stores. Format: <code>claim_name=attribute_name</
code><br><br>The keys in the map will be claim entries in the issued OIDC token, and the value of
 these claims will be the principal attribute state resulting from LDAP datastore lookup of the map
 values. If no values are returned from the LDAP datastore lookup of the attribute corresponding to
 the map value, no claim will be set in the issued OIDC token.",
          "propertyOrder" : 4800,
          "required" : false,
          "patternProperties" : {
            ".*" : {
              "type" : "string"
            }
          },
          "type" : "object",
          "exampleValue" : ""
        },
```

```
        "oidc-token-lifetime-seconds" : {
          "title" : "Token Lifetime (Seconds)",
          "description" : "",
          "propertyOrder" : 3500,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "oidc-custom-authn-context-mapper-class" : {
          "title" : "Custom Authn Context Mapper Class",
          "description" : "If issued OIDC tokens are to contain acr claims, implement the
 <code>org.forgerock.openam.sts.rest.token.provider.oidc.OpenIdConnectTokenAuthnContextMapper</code>
 interface, and specify the class name of the implementation here.",
          "propertyOrder" : 5000,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "oidc-signature-key-password" : {
          "title" : "Signature Key Password",
          "description" : "",
          "propertyOrder" : 4200,
          "required" : true,
          "type" : "string",
          "format" : "password",
          "exampleValue" : ""
        },
        "oidc-signature-key-alias" : {
          "title" : "KeyStore Signing Key Alias",
          "description" : "",
          "propertyOrder" : 4100,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "restStsDeployment" : {
      "type" : "object",
      "title" : "Deployment",
      "propertyOrder" : 1,
      "properties" : {
        "deployment-tls-offload-engine-hosts" : {
          "title" : "Trusted Remote Hosts",
          "description" : "IP addresses of TLS-Offload Hosts<br><br>Token transformation which take
 X509 Certificates as the input token require that the X509 Certificate be presented via two-way
 TLS, so that the TLS handshake can validate client certificate ownership. If OpenAM is deployed in a
 TLS-offloaded environment, in which the TLS-offloader must communicate the client certificate to the
 rest-sts via an Http header, this certificate will only be accepted if the ip address(es) of the TLS-
offload engines are specified in this list. Specify 'any' if a client certificate can be presented in
 the specified header by any rest-sts client.",
          "propertyOrder" : 1000,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
```

```
        "deployment-offloaded-two-way-tls-header-key" : {
          "title" : "Client Certificate Header Key",
          "description" : "TLS-offload host certificate header key<br><br>Token transformation
 which take X509 Certificates as the input token require that the X509 Certificate be presented
 via two-way TLS, so that the TLS handshake can validate client certificate ownership. A
 standard means of obtaining the client certificate presented via two-way TLS is via the
 javax.servlet.request.X509Certificate attribute in the ServletRequest. However, in TLS-offloaded
 deployments, the TLS-offloader must communicate the client certificate to its ultimate destination
 via an Http header. If this rest-sts instance is to support token transformations with X509
 Certificate input, and OpenAM will be deployed in a TLS-offloaded context, then this value must be
 set to the header value which the TLS-offloading engine will use to set client certificates presented
 via the TLS handshake.",
          "propertyOrder" : 900,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "deployment-auth-target-mappings" : {
          "title" : "Authentication Target Mappings",
          "description" : "Configuration of consumption of OpenAM's
 rest-authN. For each validated token type (other than OpenAM), the REST
 authN elements which will validate token instances. <br>Entry format:
 <code>TokenType;authIndexType;authIndexValue;context_key=context_value,context_key1=context_value1</
code>. <br>The <code>context_key=context_value</code> entries are optional.<br><br>Each deployed
 STS is configured with the authentication targets for each input token type for each supported
 token transformation. For example, if the transformation OPENIDCONNECT->SAML2 is supported, the
 STS instance must be configured with information specifying which elements of the OpenAM restful
 authentication context needs to be consumed to validate the OPENIDCONNECT token. The elements
 of the configuration tuple are separated by '|'. <br>The first element is the input token type
 in the token transform: i.e. X509, OPENIDCONNECT, USERNAME, or OPENAM. The second element is the
 authentication target - i.e. either 'module' or 'service', and the third element is the name of
 the authentication module or service. The fourth (optional) element provides the STS authentication
 context information about the to-be-consumed authentication context. <br>When transforming OpenID
 Connect Id tokens, the OpenID Connect authentication module must be consumed, and thus a deployed
 rest-sts instance must be configured with the name of the header/cookie element where the OpenID
 Connect Id token will be placed. For this example, the following string would define these
 configurations: <code>OPENIDCONNECT|module|oidc|oidc_id_token_auth_target_header_key=oidc_id_token</
code>. In this case, 'oidc' is the name of the OpenID Connect authentication module created to
 authenticate OpenID Connect tokens. <br>When transforming a X509 Certificate, the Certificate
 module must be consumed, and the published rest-sts instance must be configured with the name of
 the Certificate module (or the service containing the module), and the header name configured for
 the Certificate module corresponding to where the Certificate module can expect to find the to-be-
validated Certificate. The following string would define these configurations: <code>X509|module|
cert_module|x509_token_auth_target_header_key=client_cert</code>. In this case 'cert_module' is the
 name of the Certificate module, and client_cert is the header name where Certificate module has been
 configured to find the client's Certificate.",
          "propertyOrder" : 800,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "minItems" : 1,
          "type" : "array",
          "exampleValue" : ""
        }
      }
    },
    "restStsGeneral" : {
      "type" : "object",
```

```
      "title" : "General",
      "propertyOrder" : 0,
      "properties" : {
        "custom-token-providers" : {
          "title" : "Custom Token Providers",
          "description" : "If a rest-sts instance is to produce a custom token, specify
 the name of the custom token here, followed by '|', followed by the class name of the
 <code>org.forgerock.openam.sts.rest.token.provider.RestTokenProvider</code> implementation which will
 be invoked to produce an instance of the custom token.<br><br>Example: <code>MY_CUSTOM_OUTPUT_TOKEN|
org.mycompany.tokens.MyCustomTokenProvider</code> <br>Note that MY_CUSTOM_OUTPUT_TOKEN would then
 be specified as the value corresponding to the token_type key in the output_token_state json object
 specified in rest-sts token transformation invocations.",
          "propertyOrder" : 400,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "persist-issued-tokens-in-cts" : {
          "title" : "Persist Issued Tokens in Core Token Store",
          "description" : "Necessary to support token validation and cancellation<br><br>Validation of
 STS-issued tokens will involve determining whether the token has been issued, has not expired, and
 has not been cancelled. Token cancellation involves removing the record of this token from the CTS.
 Thus CTS persistence of STS-issued tokens is required to support these features.",
          "propertyOrder" : 100,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "custom-token-transforms" : {
          "title" : "Custom Token Transforms",
          "description" : "If either custom token validators or providers are specified, they must
 also be specified in a custom rest-sts token transformation. These input or output tokens can be
 specified in a transformation with standard, or other custom, tokens.<br><br>The format of these
 token transformation definitions is the same as the standard token transformation definitions.
 The first field defines the input token type, the second the output token type, and the third
 field specifies whether the OpenAM session, produced as part of the validation of the input
 token type, is invalidated following the production of the output token. <br><br>Example 1:<code>
 MY_CUSTOM_INPUT_TOKEN|SAML2|true</code> <br>Example 1 specifies a MY_CUSTOM_INPUT_TOKEN as the
 input token (requires the specification of a custom token validator) SAML2 as the produced token,
 and that the interim OpenAM Session should be invalidated after the SAML2 token is produced.
 <br><br>Example 2: <code>OPENIDCONNECT|MY_CUSTOM_OUTPUT_TOKEN|true</code> <br>Example 2 specifies
 that an OPENIDCONNECT token should be authenticated to assert the identity of a token of type
 MY_CUSTOM_OUTPUT_TOKEN (requires the specification of a custom token provider) and that the
 interim OpenAM Session should be invalidated. <br><br>Example 3: <code>MY_CUSTOM_INPUT_TOKEN|
MY_CUSTOM_OUTPUT_TOKEN|false</code> <br>Example 3 specifies that a MY_CUSTOM_INPUT_TOKEN should be
 transformed into a MY_CUSTOM_OUTPUT_TOKEN (requires the specification of both a custom provider and a
 custom validator), and that the interim OpenAM session should not be invalidated.",
          "propertyOrder" : 500,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "supported-token-transforms" : {
```

```
          "title" : "Supported Token Transformations",
          "description" : "Entry format:<code>input_token_type;output_token_type;{true|false}</
code>, where true|false indicates whether the interim OpenAM session is invalidated following token
 issuance.<br><br>Example: for the transform <code>USERNAME:SAML2</code>, it is likely that the
 OpenAM session generated as part of validating the USERNAME token should be invalidated, and thus the
 config entry would be <code>USERNAME;SAML2;true</code>. If this value is false, each USERNAME->SAML2
 transformation will result in a 'left-over' OpenAM session. Note that currently, any transformation
 which starts with an OPENAM session, e.g. <code>OPENAM;SAML2</code>,  will not invalidate this OPENAM
 session, as it was not created as part of the token transformation.",
          "propertyOrder" : 200,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "minItems" : 1,
          "type" : "array",
          "exampleValue" : ""
        },
        "custom-token-validators" : {
          "title" : "Custom Token Validators",
          "description" : "If validator of a custom token type is desired, specify
 the name of the custom token here, followed by '|', followed by the class name of the
 <code>org.forgerock.openam.sts.rest.token.validator.RestTokenTransformValidator</code> implementation
 which will be invoked to validate the custom tokens.<br><br>Example: <code>MY_CUSTOM_INPUT_TOKEN|
org.mycompany.tokens.MyCustomTokenValidator</code> <br>Note that MY_CUSTOM_INPUT_TOKEN would then
 be specified as the value corresponding to the token_type key in the input_token_state json object
 specified in rest-sts token transformation invocations.",
          "propertyOrder" : 300,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        }
      }
    }
  }
}
```

delete

Usage:

```
am> delete RESTSecurityTokenServices --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action RESTSecurityTokenServices --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action RESTSecurityTokenServices --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action RESTSecurityTokenServices --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query RESTSecurityTokenServices --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read RESTSecurityTokenServices --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update RESTSecurityTokenServices --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "restStsSaml2" : {
      "type" : "object",
      "title" : "SAML2 Token",
      "propertyOrder" : 2,
      "properties" : {
        "saml2-custom-attribute-mapper-class-name" : {
          "title" : "Custom Attribute Mapper Class Name",
          "description" : "If the class implementing attribute mapping for attributes
 contained in the issued SAML2 assertion needs to be customized, implement the
 <code>org.forgerock.openam.sts.tokengeneration.saml2.statements.AttributeMapper</code> interface, and
 specify the class name of the implementation here.",
          "propertyOrder" : 2100,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "saml2-keystore-filename" : {
          "title" : "KeystorePath",
          "description" : "Path to keystore<br><br>Provide either the full filesystem path to a
 filesystem resident keystore, or a classpath-relative path to a keystore bundled in the OpenAM .war
 file. This keystore contains the IdP public/private keys and SP public key for signed and/or
 encrypted assertions. If assertions are neither signed nor encrypted, these values need not be
 specified.",
          "propertyOrder" : 2900,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "saml2-signature-key-password" : {
          "title" : "Signature Key Password",
          "description" : "",
          "propertyOrder" : 3400,
          "required" : false,
          "type" : "string",
          "format" : "password",
          "exampleValue" : ""
        },
        "saml2-custom-authentication-statements-provider-class-name" : {
          "title" : "Custom AuthenticationStatements Class Name",
```

```
          "description" : "If the AuthenticationStatements of
 the issued SAML2 assertion need to be customized, implement the
 <code>org.forgerock.openam.sts.tokengeneration.saml2.statements.AuthenticationStatementsProvider</
code> interface, and specify the class name of the implementation here.",
          "propertyOrder" : 1800,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "saml2-encrypt-nameid" : {
          "title" : "Encrypt NameID",
          "description" : "Check this box if the assertion NameID should be encrypted. If this box is
 checked, the Encrypt Assertion box cannot be checked.",
          "propertyOrder" : 2700,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "saml2-sp-entity-id" : {
          "title" : "Service Provider Entity Id",
          "description" : "Values will be used to populate the Audiences of the AudienceRestriction
 element of the Conditions element. This value is required when issuing Bearer assertions. See section
 4.1.4.2 of Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0 for details.",
          "propertyOrder" : 1200,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "saml2-custom-attribute-statements-provider-class-name" : {
          "title" : "Custom AttributeStatements Class Name",
          "description" : "If the AttributeStatements of the
 issued SAML2 assertion need to be customized, implement the
 <code>org.forgerock.openam.sts.tokengeneration.saml2.statements.AttributeStatementsProvider</code>
 interface, and specify the class name of the implementation here.",
          "propertyOrder" : 1900,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "saml2-attribute-map" : {
          "title" : "Attribute Mappings",
          "description" : "Contains the mapping of assertion attribute names (Map
 keys) to local OpenAM attributes (Map values) in configured data stores. Format:
 <code>assertion_attr_name=ldap_attr_name</code><br><br>The DefaultAttributeMapper looks at
 profile attributes in configured data stores, or in Session properties. The keys will define
 the name of the attributes included in the Assertion Attribute statements, and the data
 pulled from the subject's directory entry or session state corresponding to the map value
 will define the value corresponding to this attribute name. The keys can have the format
 <code>[NameFomatURI|]SAML ATTRIBUTE NAME</code>. If the attribute value is enclosed in quotes,
 that quoted value will be included in the attribute without mapping. Binary attributes should be
 followed by ';binary'. <br>Examples: <ul><li>EmailAddress=mail</li><li>Address=postaladdress</
li><li>urn:oasis:names:tc:SAML:2.0:attrname-format:uri|urn:mace:dir:attribute-def:cn=cn</
li><li>partnerID=\"staticPartnerIDValue\"</li><li>urn:oasis:names:tc:SAML:2.0:attrname-format:uri|
nameID=\"staticNameIDValue\"</li><li>photo=photo;binary</li><li>urn:oasis:names:tc:SAML:2.0:attrname-
format:uri|photo=photo;binary</li></ul>",
          "propertyOrder" : 2300,
          "required" : false,
          "patternProperties" : {
            ".*" : {
```

```
              "type" : "string"
            }
          },
          "type" : "object",
          "exampleValue" : ""
        },
        "saml2-token-lifetime-seconds" : {
          "title" : "Token Lifetime (Seconds)",
          "description" : "Set to over-ride the default of 600 (10 minutes).",
          "propertyOrder" : 1500,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "saml2-keystore-password" : {
          "title" : "Keystore Password",
          "description" : "",
          "propertyOrder" : 3000,
          "required" : false,
          "type" : "string",
          "format" : "password",
          "exampleValue" : ""
        },
        "saml2-encryption-key-alias" : {
          "title" : "Encryption Key Alias",
          "description" : "This alias corresponds to the SP's x509 Certificate identified by the SP
 Entity ID for this rest-sts instance. Not necessary unless assertions are to be encrypted.",
          "propertyOrder" : 3200,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "saml2-name-id-format" : {
          "title" : "NameIdFormat",
          "description" : "The default value is <code>urn:oasis:names:tc:SAML:1.1:nameid-
format:unspecified</code><br><br>See section 8.3 of <a href=\"http://docs.oasis-open.org/security/
saml/v2.0/saml-core-2.0-os.pdf\" target=\"_blank\">Assertions and Protocols for the OASIS Security
 Assertion Markup Language (SAML) V2.0</a> for details on possible values.",
          "propertyOrder" : 1400,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "saml2-encryption-algorithm-strength" : {
          "title" : "Encryption Algorithm Strength",
          "description" : "",
          "propertyOrder" : 2850,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "saml2-signature-key-alias" : {
          "title" : "Signature Key Alias",
          "description" : "Corresponds to the private key of the IdP. Will be used to sign assertions.
 Value can remain unspecified unless assertions are signed.",
          "propertyOrder" : 3300,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
```

```
        },
        "saml2-encrypt-assertion" : {
          "title" : "Encrypt Assertion",
          "description" : "Check this box if the entire assertion should be encrypted. If this box is
 checked, the Encrypt NameID and Encrypt Attributes boxes cannot be checked.",
          "propertyOrder" : 2500,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "issuer-name" : {
          "title" : "The SAML2 Issuer Id",
          "description" : "The name of the issuer<br><br>This name will appear in some issued tokens -
 e.g. in the <code>saml:Issuer</code> of issued SAML2 assertions.",
          "propertyOrder" : 1100,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "saml2-sign-assertion" : {
          "title" : "Sign Assertion",
          "description" : "",
          "propertyOrder" : 2400,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "saml2-custom-conditions-provider-class-name" : {
          "title" : "Custom Conditions Provider Class Name",
          "description" : "If the Conditions of the issued SAML2 assertion need to be customized,
 implement the <code>org.forgerock.openam.sts.tokengeneration.saml2.statements.ConditionsProvider</
code> interface, and specify the class name of the implementation here.",
          "propertyOrder" : 1600,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "saml2-encrypt-attributes" : {
          "title" : "Encrypt Attributes",
          "description" : "Check this box if the assertion Attributes should be encrypted. If this box
 is checked, the Encrypt Assertion box cannot be checked.",
          "propertyOrder" : 2600,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "saml2-custom-subject-provider-class-name" : {
          "title" : "Customs Subject Provider Class Name",
          "description" : "If the Subject of the issued SAML2 assertion needs to be customized,
 implement the <code>org.forgerock.openam.sts.tokengeneration.saml2.statements.SubjectProvider</code>
 interface, and specify the class name of the implementation here.",
          "propertyOrder" : 1700,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "saml2-custom-authz-decision-statements-provider-class-name" : {
          "title" : "Custom Authorization Decision Statements Class Name",
```

```
          "description" : "If the AuthorizationDecisionStatements
 of the issued SAML2 assertion need to be customized, implement the
 <code>org.forgerock.openam.sts.tokengeneration.saml2.statements.AuthzDecisionStatementsProvider</
code> interface, and specify the class name of the implementation here.",
          "propertyOrder" : 2000,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "saml2-key-transport-algorithm" : {
          "title" : "Key Transport Algorithm",
          "description" : "This setting controls the encryption algorithm used to encrypt the
 symmetric encryption key when SAML2 token encryption is enabled. Valid values include: <pre>http://
www.w3.org/2001/04/xmlenc#rsa-1_5</pre>, <pre>http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p</pre>,
 and <pre>http://www.w3.org/2009/xmlenc11#rsa-oaep</pre>",
          "propertyOrder" : 2860,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "saml2-custom-authn-context-mapper-class-name" : {
          "title" : "Custom Authentication Context Class Name",
          "description" : "If the AuthnContext mapping implemented by the
 <code>org.forgerock.openam.sts.rest.token.provider.saml.DefaultSaml2JsonTokenAuthnContextMapper</
code> class needs to be customized, implement the
 <code>org.forgerock.openam.sts.rest.token.provider.saml.Saml2JsonTokenAuthnContextMapper</code>
 interface, and specify the name of the implementation here.",
          "propertyOrder" : 2200,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "saml2-encryption-algorithm" : {
          "title" : "Encryption Algorithm",
          "description" : "Algorithm used to encrypt generated assertions.",
          "propertyOrder" : 2800,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "saml2-sp-acs-url" : {
          "title" : "Service Provider Assertion Consumer Service Url",
          "description" : "When issuing bearer assertions, the recipient attribute of the
 SubjectConfirmation element must be set to the Service Provider Assertion Consumer Service Url. See
 section 4.1.4.2 of Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0 for details.
 Value required when issuing Bearer assertions.",
          "propertyOrder" : 1300,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "restStsOidc" : {
      "type" : "object",
      "title" : "OpenID Connect Token",
      "propertyOrder" : 3,
      "properties" : {
        "oidc-authorized-party" : {
```

```
          "title" : "Authorized Party",
          "description" : "",
          "propertyOrder" : 4700,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "oidc-signature-algorithm" : {
          "title" : "Token Signature Algorithm",
          "description" : "Algorithm used to sign issued OIDC tokens",
          "propertyOrder" : 3600,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "oidc-issuer" : {
          "title" : "The OpenID Connect Token Provider Issuer Id",
          "description" : "",
          "propertyOrder" : 3450,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "oidc-custom-authn-method-references-mapper-class" : {
          "title" : "Custom Authn Methods References Mapper Class",
          "description" : "If issued OIDC tokens are to contain amr claims, implement the
 <code>org.forgerock.openam.sts.rest.token.provider.oidc.OpenIdConnectTokenAuthMethodReferencesMapper</
code> interface, and specify the class name of the implementation here.",
          "propertyOrder" : 5100,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "oidc-custom-claim-mapper-class" : {
          "title" : "Custom Claim Mapper Class",
          "description" : "If the class implementing attribute mapping for attributes
 contained in issued OpenID Connect tokens needs to be customized, implement the
 <code>org.forgerock.openam.sts.tokengeneration.oidc.OpenIdConnectTokenClaimMapper</code> interface,
 and specify the class name of the implementation here.",
          "propertyOrder" : 4900,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "oidc-keystore-password" : {
          "title" : "KeyStore Password",
          "description" : "",
          "propertyOrder" : 3900,
          "required" : true,
          "type" : "string",
          "format" : "password",
          "exampleValue" : ""
        },
        "oidc-client-secret" : {
          "title" : "Client Secret",
          "description" : "For HMAC-signed tokens, the client secret used as the HMAC key.<br><br>For
 HMAC-signed tokens, the KeyStore location, password, signature key alias and password configurations
 are not required.",
          "propertyOrder" : 4400,
```

```
          "required" : true,
          "type" : "string",
          "format" : "password",
          "exampleValue" : ""
        },
        "oidc-public-key-reference-type" : {
          "title" : "Public Key Reference Type",
          "description" : "For tokens signed with RSA, how should corresponding public key be
 referenced in the issued jwt",
          "propertyOrder" : 3700,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "oidc-audience" : {
          "title" : "Issued Tokens Audience",
          "description" : "Contents will be set in the aud claim",
          "propertyOrder" : 4600,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "oidc-keystore-location" : {
          "title" : "KeyStore Location",
          "description" : "For RSA-signed tokens, the filesystem or classpath location of the KeyStore
 containing signing key entry<br><br>For RSA-signed tokens, the KeyStore location, password, signing-
key alias, and signing key password must be specified. The client secret is not required for RSA-
signed tokens.",
          "propertyOrder" : 3800,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "oidc-claim-map" : {
          "title" : "Claim Map",
          "description" : "Contains the mapping of OIDC token claim names (Map keys) to local
 OpenAM attributes (Map values) in configured data stores. Format: <code>claim_name=attribute_name</
code><br><br>The keys in the map will be claim entries in the issued OIDC token, and the value of
 these claims will be the principal attribute state resulting from LDAP datastore lookup of the map
 values. If no values are returned from the LDAP datastore lookup of the attribute corresponding to
 the map value, no claim will be set in the issued OIDC token.",
          "propertyOrder" : 4800,
          "required" : false,
          "patternProperties" : {
            ".*" : {
              "type" : "string"
            }
          },
          "type" : "object",
          "exampleValue" : ""
        },
        "oidc-token-lifetime-seconds" : {
          "title" : "Token Lifetime (Seconds)",
          "description" : "",
          "propertyOrder" : 3500,
          "required" : false,
```

```
          "type" : "integer",
          "exampleValue" : ""
        },
        "oidc-custom-authn-context-mapper-class" : {
          "title" : "Custom Authn Context Mapper Class",
          "description" : "If issued OIDC tokens are to contain acr claims, implement the
 <code>org.forgerock.openam.sts.rest.token.provider.oidc.OpenIdConnectTokenAuthnContextMapper</code>
 interface, and specify the class name of the implementation here.",
          "propertyOrder" : 5000,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "oidc-signature-key-password" : {
          "title" : "Signature Key Password",
          "description" : "",
          "propertyOrder" : 4200,
          "required" : true,
          "type" : "string",
          "format" : "password",
          "exampleValue" : ""
        },
        "oidc-signature-key-alias" : {
          "title" : "KeyStore Signing Key Alias",
          "description" : "",
          "propertyOrder" : 4100,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "restStsDeployment" : {
      "type" : "object",
      "title" : "Deployment",
      "propertyOrder" : 1,
      "properties" : {
        "deployment-tls-offload-engine-hosts" : {
          "title" : "Trusted Remote Hosts",
          "description" : "IP addresses of TLS-Offload Hosts<br><br>Token transformation which take
 X509 Certificates as the input token require that the X509 Certificate be presented via two-way
 TLS, so that the TLS handshake can validate client certificate ownership. If OpenAM is deployed in a
 TLS-offloaded environment, in which the TLS-offloader must communicate the client certificate to the
 rest-sts via an Http header, this certificate will only be accepted if the ip address(es) of the TLS-
offload engines are specified in this list. Specify 'any' if a client certificate can be presented in
 the specified header by any rest-sts client.",
          "propertyOrder" : 1000,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "deployment-offloaded-two-way-tls-header-key" : {
          "title" : "Client Certificate Header Key",
          "description" : "TLS-offload host certificate header key<br><br>Token transformation
 which take X509 Certificates as the input token require that the X509 Certificate be presented
 via two-way TLS, so that the TLS handshake can validate client certificate ownership. A
```

```
 standard means of obtaining the client certificate presented via two-way TLS is via the
 javax.servlet.request.X509Certificate attribute in the ServletRequest. However, in TLS-offloaded
 deployments, the TLS-offloader must communicate the client certificate to its ultimate destination
 via an Http header. If this rest-sts instance is to support token transformations with X509
 Certificate input, and OpenAM will be deployed in a TLS-offloaded context, then this value must be
 set to the header value which the TLS-offloading engine will use to set client certificates presented
 via the TLS handshake.",
          "propertyOrder" : 900,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "deployment-auth-target-mappings" : {
          "title" : "Authentication Target Mappings",
          "description" : "Configuration of consumption of OpenAM's
 rest-authN. For each validated token type (other than OpenAM), the REST
 authN elements which will validate token instances. <br>Entry format:
 <code>TokenType;authIndexType;authIndexValue;context_key=context_value,context_key1=context_value1</
code>. <br>The <code>context_key=context_value</code> entries are optional.<br><br>Each deployed
 STS is configured with the authentication targets for each input token type for each supported
 token transformation. For example, if the transformation OPENIDCONNECT->SAML2 is supported, the
 STS instance must be configured with information specifying which elements of the OpenAM restful
 authentication context needs to be consumed to validate the OPENIDCONNECT token. The elements
 of the configuration tuple are separated by '|'. <br>The first element is the input token type
 in the token transform: i.e. X509, OPENIDCONNECT, USERNAME, or OPENAM. The second element is the
 authentication target - i.e. either 'module' or 'service', and the third element is the name of
 the authentication module or service. The fourth (optional) element provides the STS authentication
 context information about the to-be-consumed authentication context. <br>When transforming OpenID
 Connect Id tokens, the OpenID Connect authentication module must be consumed, and thus a deployed
 rest-sts instance must be configured with the name of the header/cookie element where the OpenID
 Connect Id token will be placed. For this example, the following string would define these
 configurations: <code>OPENIDCONNECT|module|oidc|oidc_id_token_auth_target_header_key=oidc_id_token</
code>. In this case, 'oidc' is the name of the OpenID Connect authentication module created to
 authenticate OpenID Connect tokens. <br>When transforming a X509 Certificate, the Certificate
 module must be consumed, and the published rest-sts instance must be configured with the name of
 the Certificate module (or the service containing the module), and the header name configured for
 the Certificate module corresponding to where the Certificate module can expect to find the to-be-
validated Certificate. The following string would define these configurations: <code>X509|module|
cert_module|x509_token_auth_target_header_key=client_cert</code>. In this case 'cert_module' is the
 name of the Certificate module, and client_cert is the header name where Certificate module has been
 configured to find the client's Certificate.",
          "propertyOrder" : 800,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "minItems" : 1,
          "type" : "array",
          "exampleValue" : ""
        }
      }
    },
    "restStsGeneral" : {
      "type" : "object",
      "title" : "General",
      "propertyOrder" : 0,
      "properties" : {
        "custom-token-providers" : {
          "title" : "Custom Token Providers",
```

```
          "description" : "If a rest-sts instance is to produce a custom token, specify
 the name of the custom token here, followed by '|', followed by the class name of the
 <code>org.forgerock.openam.sts.rest.token.provider.RestTokenProvider</code> implementation which will
 be invoked to produce an instance of the custom token.<br><br>Example: <code>MY_CUSTOM_OUTPUT_TOKEN|
org.mycompany.tokens.MyCustomTokenProvider</code> <br>Note that MY_CUSTOM_OUTPUT_TOKEN would then
 be specified as the value corresponding to the token_type key in the output_token_state json object
 specified in rest-sts token transformation invocations.",
          "propertyOrder" : 400,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "persist-issued-tokens-in-cts" : {
          "title" : "Persist Issued Tokens in Core Token Store",
          "description" : "Necessary to support token validation and cancellation<br><br>Validation of
 STS-issued tokens will involve determining whether the token has been issued, has not expired, and
 has not been cancelled. Token cancellation involves removing the record of this token from the CTS.
 Thus CTS persistence of STS-issued tokens is required to support these features.",
          "propertyOrder" : 100,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "custom-token-transforms" : {
          "title" : "Custom Token Transforms",
          "description" : "If either custom token validators or providers are specified, they must
 also be specified in a custom rest-sts token transformation. These input or output tokens can be
 specified in a transformation with standard, or other custom, tokens.<br><br>The format of these
 token transformation definitions is the same as the standard token transformation definitions.
 The first field defines the input token type, the second the output token type, and the third
 field specifies whether the OpenAM session, produced as part of the validation of the input
 token type, is invalidated following the production of the output token. <br><br>Example 1:<code>
 MY_CUSTOM_INPUT_TOKEN|SAML2|true</code> <br>Example 1 specifies a MY_CUSTOM_INPUT_TOKEN as the
 input token (requires the specification of a custom token validator) SAML2 as the produced token,
 and that the interim OpenAM Session should be invalidated after the SAML2 token is produced.
 <br><br>Example 2: <code>OPENIDCONNECT|MY_CUSTOM_OUTPUT_TOKEN|true</code> <br>Example 2 specifies
 that an OPENIDCONNECT token should be authenticated to assert the identity of a token of type
 MY_CUSTOM_OUTPUT_TOKEN (requires the specification of a custom token provider) and that the
 interim OpenAM Session should be invalidated. <br><br>Example 3: <code>MY_CUSTOM_INPUT_TOKEN|
MY_CUSTOM_OUTPUT_TOKEN|false</code> <br>Example 3 specifies that a MY_CUSTOM_INPUT_TOKEN should be
 transformed into a MY_CUSTOM_OUTPUT_TOKEN (requires the specification of both a custom provider and a
 custom validator), and that the interim OpenAM session should not be invalidated.",
          "propertyOrder" : 500,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "supported-token-transforms" : {
          "title" : "Supported Token Transformations",
          "description" : "Entry format:<code>input_token_type;output_token_type;{true|false}</
code>, where true|false indicates whether the interim OpenAM session is invalidated following token
 issuance.<br><br>Example: for the transform <code>USERNAME:SAML2</code>, it is likely that the
 OpenAM session generated as part of validating the USERNAME token should be invalidated, and thus the
```

```
 config entry would be <code>USERNAME;SAML2;true</code>. If this value is false, each USERNAME->SAML2
 transformation will result in a 'left-over' OpenAM session. Note that currently, any transformation
 which starts with an OPENAM session, e.g. <code>OPENAM;SAML2</code>,  will not invalidate this OPENAM
 session, as it was not created as part of the token transformation.",
          "propertyOrder" : 200,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "minItems" : 1,
          "type" : "array",
          "exampleValue" : ""
        },
        "custom-token-validators" : {
          "title" : "Custom Token Validators",
          "description" : "If validator of a custom token type is desired, specify
 the name of the custom token here, followed by '|', followed by the class name of the
 <code>org.forgerock.openam.sts.rest.token.validator.RestTokenTransformValidator</code> implementation
 which will be invoked to validate the custom tokens.<br><br>Example: <code>MY_CUSTOM_INPUT_TOKEN|
org.mycompany.tokens.MyCustomTokenValidator</code> <br>Note that MY_CUSTOM_INPUT_TOKEN would then
 be specified as the value corresponding to the token_type key in the input_token_state json object
 specified in rest-sts token transformation invocations.",
          "propertyOrder" : 300,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        }
      }
    }
  }
}
```

RadiusClient

Global Operations

Resource path: `/global-config/services/RadiusServerService/radiusClient`

Resource version: `1.0`

create

Usage:

```
am> create RadiusClient --global --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "clientIpAddress" : {
      "title" : "Client IP Address",
      "description" : "The IP Address of the client.<br><br><a href=\"http://tools.ietf.org/html/
rfc2865#section-5.4\" target=\"_blank\">Section 5.4 of the RADIUS Authentication Specification,
 RFC 2865</a>, indicates that the source IP address of the Access-Request packet <em>MUST</em> be
 used to identify a configured client and hence determine the shared secret to use for decrypting
 the User-Password field.<p><p>This property should hold the source IP address of the client. This
 should match the value obtained from Java's <code>InetSocketAddress.getAddress().toString()</code>
 function.<p><p>To verify the value, send an Access-Request packet to OpenAM's RADIUS port and watch
 for a message stating: <code>\"No Defined RADIUS Client matches IP address '/127.0.0.1'. Dropping
 request.\"</code>. The value used in this property should match the IP address returned in the single
 quotes.",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "clientSecret" : {
      "title" : "Client Secret",
      "description" : "This secret shared between server and client for encryption of the user
 password.<br><br>This secret must be conveyed to the RADIUS client and entered into its configuration
 before the User-Password field of incoming Access-Request packets can be decrypted to validate the
 password for the represented by that packet.",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "string",
      "format" : "password",
      "exampleValue" : ""
    },
    "handlerClass" : {
      "title" : "Handler Class",
      "description" : "The fully qualified name of a class to handle incoming
 RADIUS Access-Requests for this client.<br><br>This class must implement the
 <code>com.sun.identity.authentication.modules.radius.server.spi.AccessRequestHandler</code> interface
 to handle incoming Access-Request packets and provide a suitable response. An instance of this class
 is created when configuration is first loaded to validate the class and then once for each new
 request. The configuration properties will only be passed for the request handling instances and not
 when validating the class.",
      "propertyOrder" : 700,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "handlerConfig" : {
      "title" : "Handler Class Configuration Properties",
      "description" : "Properties needed by the handler class for its configuration.<br><br>These
 properties are provided to the handler via its <code>init</code> method prior to the call to handle
```

```
 the request packet. If these values are changed the next handler instance created for an incoming
 request will receive the updated values. Each entry assumes that the first '<code>=</code>' character
 incurred separates a key from its value. All entries are placed in a properties file handed to each
 handler instance.",
      "propertyOrder" : 900,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "clientPacketsLogged" : {
      "title" : "Log Packet Contents for this Client",
      "description" : "Indicates if full packet contents should be dumped to the log.<br><br>When
 troubleshooting issues with RADIUS it is helpful to know what was received in a given packet.
 Enabling this feature will cause packet contents to be logged in a human consumable format. The only
 caveat is that the USER_PASSWORD field will be obfiscated by replacing with asterisks. This should
 only be enabled for troubleshooting as it adds significant content to logs and slows processing.",
      "propertyOrder" : 500,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
```

delete

Usage:

```
am> delete RadiusClient --global --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action RadiusClient --global --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action RadiusClient --global --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action RadiusClient --global --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query RadiusClient --global --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read RadiusClient --global --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update RadiusClient --global --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "clientIpAddress" : {
      "title" : "Client IP Address",
      "description" : "The IP Address of the client.<br><br><a href=\"http://tools.ietf.org/html/
rfc2865#section-5.4\" target=\"_blank\">Section 5.4 of the RADIUS Authentication Specification,
 RFC 2865</a>, indicates that the source IP address of the Access-Request packet <em>MUST</em> be
 used to identify a configured client and hence determine the shared secret to use for decrypting
 the User-Password field.<p><p>This property should hold the source IP address of the client. This
 should match the value obtained from Java's <code>InetSocketAddress.getAddress().toString()</code>
 function.<p><p>To verify the value, send an Access-Request packet to OpenAM's RADIUS port and watch
 for a message stating: <code>\"No Defined RADIUS Client matches IP address '/127.0.0.1'. Dropping
 request.\"</code>. The value used in this property should match the IP address returned in the single
 quotes.",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "clientSecret" : {
      "title" : "Client Secret",
      "description" : "This secret shared between server and client for encryption of the user
 password.<br><br>This secret must be conveyed to the RADIUS client and entered into its configuration
 before the User-Password field of incoming Access-Request packets can be decrypted to validate the
 password for the represented by that packet.",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "string",
      "format" : "password",
      "exampleValue" : ""
    },
    "handlerClass" : {
      "title" : "Handler Class",
      "description" : "The fully qualified name of a class to handle incoming
 RADIUS Access-Requests for this client.<br><br>This class must implement the
 <code>com.sun.identity.authentication.modules.radius.server.spi.AccessRequestHandler</code> interface
 to handle incoming Access-Request packets and provide a suitable response. An instance of this class
 is created when configuration is first loaded to validate the class and then once for each new
 request. The configuration properties will only be passed for the request handling instances and not
 when validating the class.",
      "propertyOrder" : 700,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "handlerConfig" : {
      "title" : "Handler Class Configuration Properties",
      "description" : "Properties needed by the handler class for its configuration.<br><br>These
 properties are provided to the handler via its <code>init</code> method prior to the call to handle
 the request packet. If these values are changed the next handler instance created for an incoming
 request will receive the updated values. Each entry assumes that the first '<code>=</code>' character
 incurred separates a key from its value. All entries are placed in a properties file handed to each
 handler instance.",
      "propertyOrder" : 900,
```

```
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "clientPacketsLogged" : {
      "title" : "Log Packet Contents for this Client",
      "description" : "Indicates if full packet contents should be dumped to the log.<br><br>When
 troubleshooting issues with RADIUS it is helpful to know what was received in a given packet.
 Enabling this feature will cause packet contents to be logged in a human consumable format. The only
 caveat is that the USER_PASSWORD field will be obfiscated by replacing with asterisks. This should
 only be enabled for troubleshooting as it adds significant content to logs and slows processing.",
      "propertyOrder" : 500,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
```

RadiusModule

Realm Operations

Resource path: `/realm-config/authentication/modules/radius`

Resource version: `1.0`

create

Usage:

```
am> create RadiusModule --realm Realm --id id --body body
```

Parameters:

`--id`

The unique identifier for the resource.

`--body`

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "healthCheckInterval" : {
      "title" : "Health check interval",
```

```
      "description" : "The interval between checks to unavailable RADIUS servers, in minutes.
 <br><br>Determines how often AM checks an offline server's status. The check will send an invalid
 authentication request to the RADIUS server. Offline servers will not be used until the healthcheck
 was successful. Primary servers that become available will be used in preference to secondary
 servers.",
      "propertyOrder" : 600,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "serverTimeout" : {
      "title" : "Timeout",
      "description" : "Amount of time in seconds to wait for the RADIUS server response.<br><br>This
 sets the <code>SO_TIMEOUT</code> timeout on the packet. ",
      "propertyOrder" : 500,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "sharedSecret" : {
      "title" : "Shared Secret",
      "description" : "The secret shared between the RADIUS server and the authentication module.",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "string",
      "format" : "password",
      "exampleValue" : ""
    },
    "authenticationLevel" : {
      "title" : "Authentication Level",
      "description" : "The authentication level associated with this module.<br><br>Each
 authentication module has an authentication level that can be used to indicate the level of security
 associated with the module; 0 is the lowest (and the default). ",
      "propertyOrder" : 700,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "serverPortNumber" : {
      "title" : "Port Number",
      "description" : "Port number on which the RADIUS server is listening.",
      "propertyOrder" : 400,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "primaryRadiusServers" : {
      "title" : "Primary Radius Servers",
      "description" : "A list of primary Radius servers that will be used for
 authentication<br><br>The module will use these servers in preference to the secondary servers. For
 a single entry, specify the IP address or fully qualified domain name of the Radius server.<br/><br/
>Multiple entries allow associations between AM servers and a Radius server. The format is:<br/><br/
><code>local server name | radius_server</code><br/><br/><i>NB </i>The local server name is the full
 name of the server from the list of servers and sites.",
      "propertyOrder" : 100,
      "required" : true,
      "items" : {
        "type" : "string"
      },
```

```
      "type" : "array",
      "exampleValue" : ""
    },
    "secondaryRadiusServers" : {
      "title" : "Secondary Radius Servers",
      "description" : "A list of secondary Radius servers that will be used for authentication,
 in case the primary servers are unavailable.<br><br>The module will use secondary servers for
 authentication if all primary servers are unavailable. For a single entry, specify the IP address,
 or fully qualified domain name of the Radius server.<br/><br/>Multiple entries allow associations
 between AM servers and a Radius server. The format is:<br/><br/><code>local server name |
 radius_server</code><br/><br/><i>NB </i>The local server name is the full name of the server from the
 list of servers and sites.",
      "propertyOrder" : 200,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    }
  }
}
```

delete

Usage:

```
am> delete RadiusModule --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action RadiusModule --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action RadiusModule --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action RadiusModule --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query RadiusModule --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read RadiusModule --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update RadiusModule --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "healthCheckInterval" : {
      "title" : "Health check interval",
      "description" : "The interval between checks to unavailable RADIUS servers, in minutes.
<br><br>Determines how often AM checks an offline server's status. The check will send an invalid
authentication request to the RADIUS server. Offline servers will not be used until the healthcheck
was successful. Primary servers that become available will be used in preference to secondary
servers.",
      "propertyOrder" : 600,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "serverTimeout" : {
      "title" : "Timeout",
      "description" : "Amount of time in seconds to wait for the RADIUS server response.<br><br>This
sets the <code>SO_TIMEOUT</code> timeout on the packet. ",
      "propertyOrder" : 500,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "sharedSecret" : {
      "title" : "Shared Secret",
      "description" : "The secret shared between the RADIUS server and the authentication module.",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "string",
      "format" : "password",
      "exampleValue" : ""
    },
    "authenticationLevel" : {
      "title" : "Authentication Level",
      "description" : "The authentication level associated with this module.<br><br>Each
authentication module has an authentication level that can be used to indicate the level of security
associated with the module; 0 is the lowest (and the default). ",
      "propertyOrder" : 700,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "serverPortNumber" : {
      "title" : "Port Number",
      "description" : "Port number on which the RADIUS server is listening.",
      "propertyOrder" : 400,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "primaryRadiusServers" : {
      "title" : "Primary Radius Servers",
      "description" : "A list of primary Radius servers that will be used for
authentication<br><br>The module will use these servers in preference to the secondary servers. For
```

```
 a single entry, specify the IP address or fully qualified domain name of the Radius server.<br/><br/
>Multiple entries allow associations between AM servers and a Radius server. The format is:<br/><br/
><code>local server name | radius_server</code><br/><br/><i>NB </i>The local server name is the full
 name of the server from the list of servers and sites.",
      "propertyOrder" : 100,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "secondaryRadiusServers" : {
      "title" : "Secondary Radius Servers",
      "description" : "A list of secondary Radius servers that will be used for authentication,
 in case the primary servers are unavailable.<br><br>The module will use secondary servers for
 authentication if all primary servers are unavailable. For a single entry, specify the IP address,
 or fully qualified domain name of the Radius server.<br/><br/>Multiple entries allow associations
 between AM servers and a Radius server. The format is:<br/><br/><code>local server name |
 radius_server</code><br/><br/><i>NB </i>The local server name is the full name of the server from the
 list of servers and sites.",
      "propertyOrder" : 200,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    }
  }
}
```

Global Operations

Resource path: `/global-config/authentication/modules/radius`

Resource version: `1.0`

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action RadiusModule --global --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action RadiusModule --global --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action RadiusModule --global --actionName nextdescendents
```

read

Usage:

```
am> read RadiusModule --global
```

update

Usage:

```
am> update RadiusModule --global --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "defaults" : {
      "properties" : {
        "sharedSecret" : {
          "title" : "Shared Secret",
          "description" : "The secret shared between the RADIUS server and the authentication
 module.",
          "propertyOrder" : 300,
          "required" : true,
          "type" : "string",
          "format" : "password",
          "exampleValue" : ""
        },
        "secondaryRadiusServers" : {
          "title" : "Secondary Radius Servers",
          "description" : "A list of secondary Radius servers that will be used for authentication,
 in case the primary servers are unavailable.<br><br>The module will use secondary servers for
 authentication if all primary servers are unavailable. For a single entry, specify the IP address,
 or fully qualified domain name of the Radius server.<br/><br/>Multiple entries allow associations
 between AM servers and a Radius server. The format is:<br/><br/><code>local server name |
 radius_server</code><br/><br/><i>NB </i>The local server name is the full name of the server from the
 list of servers and sites.",
          "propertyOrder" : 200,
          "required" : true,
          "items" : {
            "type" : "string"
```

```
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "serverTimeout" : {
          "title" : "Timeout",
          "description" : "Amount of time in seconds to wait for the RADIUS server
 response.<br><br>This sets the <code>SO_TIMEOUT</code> timeout on the packet. ",
          "propertyOrder" : 500,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "authenticationLevel" : {
          "title" : "Authentication Level",
          "description" : "The authentication level associated with this module.<br><br>Each
 authentication module has an authentication level that can be used to indicate the level of security
 associated with the module; 0 is the lowest (and the default). ",
          "propertyOrder" : 700,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "serverPortNumber" : {
          "title" : "Port Number",
          "description" : "Port number on which the RADIUS server is listening.",
          "propertyOrder" : 400,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "primaryRadiusServers" : {
          "title" : "Primary Radius Servers",
          "description" : "A list of primary Radius servers that will be used for
 authentication<br><br>The module will use these servers in preference to the secondary servers. For
 a single entry, specify the IP address or fully qualified domain name of the Radius server.<br/><br/
>Multiple entries allow associations between AM servers and a Radius server. The format is:<br/><br/
><code>local server name | radius_server</code><br/><br/><i>NB </i>The local server name is the full
 name of the server from the list of servers and sites.",
          "propertyOrder" : 100,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "healthCheckInterval" : {
          "title" : "Health check interval",
          "description" : "The interval between checks to unavailable RADIUS servers, in minutes.
 <br><br>Determines how often AM checks an offline server's status. The check will send an invalid
 authentication request to the RADIUS server. Offline servers will not be used until the healthcheck
 was successful. Primary servers that become available will be used in preference to secondary
 servers.",
          "propertyOrder" : 600,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        }
```

```
      },
      "type" : "object",
      "title" : "Realm Defaults"
    }
  }
}
```

RadiusServer

Global Operations

Resource path: `/global-config/services/RadiusServerService`

Resource version: `1.0`

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action RadiusServer --global --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action RadiusServer --global --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action RadiusServer --global --actionName nextdescendents
```

read

Usage:

```
am> read RadiusServer --global
```

update

Usage:

```
am> update RadiusServer --global --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "radiusThreadPoolQueueSize" : {
      "title" : "Thread Pool Queue Size",
      "description" : "The number of requests that can be queued for the pool before further requests
 will be silently dropped. See also \"Thread Pool Core Size\" and \"Thread Pool Max Size\". Specify a
 value from <code>1</code> to <code>1000</code>.",
      "propertyOrder" : 1100,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "radiusThreadPoolMaxSize" : {
      "title" : "Thread Pool Max Size",
      "description" : "Maximum number of threads allowed in the pool. See also \"Thread Pool Core Size
\".",
      "propertyOrder" : 800,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "radiusThreadPoolKeepaliveSeconds" : {
      "title" : "Thread Pool Keep-Alive Seconds",
      "description" : "If the pool currently has more than Thread Pool Core Size threads, excess
 threads will be terminated if they have been idle for more than the Keep-Alive Seconds. Specify a
 value from <code>1</code> to <code>3600</code>.",
      "propertyOrder" : 1000,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "radiusListenerEnabled" : {
      "title" : "Enabled",
      "description" : "Enables the OpenAM RADIUS server to listen for requests on the listener port
 and to handle the requests.",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "radiusThreadPoolCoreSize" : {
      "title" : "Thread Pool Core Size",
      "description" : "When a RADIUS request is received and fewer than <code>corePoolSize</code>
 threads are running, a new thread is created to handle the request, even if other worker threads are
```

```
 idle. If there are more than \"Thread Pool Core Size\" but less than \"Thread Pool Max Size\" threads
 running, a new thread will be created only if the queue is full. By setting \"Thread Pool Core Size\"
 and \"Thread Pool Max Size\" to the same value, you create a fixed-size thread pool. Specify a value
 from <code>1</code> to <code>100</code>.",
      "propertyOrder" : 600,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "radiusServerPort" : {
      "title" : "Listener Port",
      "description" : "The UDP port on which each OpenAM server will listen for RADIUS Access-Request
 packets<br><br>According to the RADIUS Authentication Specification, <a href=\"http://tools.ietf.org/
html/rfc2865\" target=\"_blank\">RFC 2865</a>, the officially assigned port number for RADIUS is
 <code>1812</code>. Specify a value from <code>1024</code> to <code>65535</code>. All client requests
 are handled through the same port.",
      "propertyOrder" : 400,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    }
  }
}
```

Realms

Global Operations

The endpoint for Realm operations

Resource path: `/global-config/realms`

Resource version: `1.0`

create

Create a Realm

Usage:

```
am> create Realms --global --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "$schema" : "http://json-schema.org/draft-04/schema#",
  "description" : "Represents a Realm Resource",
  "type" : "object",
```

```
  "title" : "Realm",
  "properties" : {
    "name" : {
      "type" : "string",
      "title" : "Name",
      "description" : "The name of the Realm"
    },
    "active" : {
      "type" : "boolean",
      "title" : "Active",
      "description" : "True if the Realm is active"
    },
    "parentPath" : {
      "type" : "string",
      "title" : "Parent",
      "description" : "The path of the Realm's parent Realm"
    },
    "aliases" : {
      "type" : "array",
      "title" : "Aliases",
      "description" : "Aliases which can be used reference to the Realm",
      "items" : {
        "type" : "string"
      }
    }
  },
  "required" : [ "name", "active", "parentPath", "aliases" ]
}
```

delete

Delete a Realm

Usage:

```
am> delete Realms --global --id id
```

Parameters:

--id

The unique identifier for the resource.

query

Usage:

```
am> query Realms --global --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Read a Realm

Usage:

```
am> read Realms --global --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Update a Realm

Usage:

```
am> update Realms --global --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "$schema" : "http://json-schema.org/draft-04/schema#",
  "description" : "Represents a Realm Resource",
  "type" : "object",
  "title" : "Realm",
  "properties" : {
    "name" : {
      "type" : "string",
      "title" : "Name",
      "description" : "The name of the Realm"
    },
    "active" : {
      "type" : "boolean",
      "title" : "Active",
      "description" : "True if the Realm is active"
    },
    "parentPath" : {
      "type" : "string",
      "title" : "Parent",
      "description" : "The path of the Realm's parent Realm"
    },
    "aliases" : {
      "type" : "array",
      "title" : "Aliases",
      "description" : "Aliases which can be used reference to the Realm",
```

```
      "items" : {
        "type" : "string"
      }
    }
  },
  "required" : [ "name", "active", "parentPath", "aliases" ]
}
```

Records

Realm Operations

Service for creating records.

Resource path: `/records`

Resource version: `1.0`

start

Starts recording.

Usage:

```
am> action Records --realm Realm --body body --actionName start
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "description" : "The properties of a Record, which can deserialized from json.",
  "type" : "object",
  "title" : "Record properties",
  "properties" : {
    "issueID" : {
      "description" : "A case number is a good choice for the issueID value.",
      "title" : "Issue ID",
      "type" : "integer",
      "format" : "int64"
    },
    "referenceID" : {
      "description" : "A second identifier to segregate multiple recording events for the same
 issue.",
      "title" : "Reference ID",
      "type" : "string"
    },
    "description" : {
      "description" : "A textual description of the recording event.",
      "title" : "Description",
      "type" : "string"
```

```
    },
    "threadDump" : {
      "description" : "Object used to specify thread dump settings.",
      "title" : "Thread dump settings",
      "type" : "object",
      "properties" : {
        "enable" : {
          "description" : "Whether to dump threads during the recording event.",
          "title" : "Thread dump enabled",
          "type" : "boolean"
        },
        "delay" : {
          "description" : "Object used to specify an interval at which thread dumps are taken. The
initial thread dump is taken at the start of the recording event; subsequent thread dumps are taken
at multiples of the delay interval.",
          "title" : "Thread dump delay",
          "type" : "object",
          "properties" : {
            "timeUnit" : {
              "description" : "The time unit being used to specify the delay for the thread dumps.",
              "title" : "Thread dump delay time unit",
              "type" : "string",
              "enum" : [ "DAYS", "HOURS", "MINUTES", "SECONDS", "MILLISECONDS", "MICROSECONDS",
"NANOSECONDS" ]
            },
            "value" : {
              "description" : "The value for the thread dump delay, in the specified thread dump delay
time unit. The initial thread dump is taken at the start of the recording event; subsequent thread
dumps are taken at multiples of the delay interval.",
              "title" : "Thread dump delay value",
              "type" : "integer",
              "format" : "int64"
            }
          }
        }
      }
    },
    "configExport" : {
      "description" : "Configuration Export properties.",
      "title" : "Configuration export properties",
      "type" : "object",
      "properties" : {
        "enable" : {
          "description" : "Whether to export the OpenAM configuration upon completion of the recording
event.",
          "title" : "Config export enabled",
          "type" : "boolean"
        },
        "password" : {
          "description" : "A key required to import the exported configuration.",
          "title" : "Config export password",
          "type" : "string"
        },
        "sharePassword" : {
          "description" : "Whether to show the password value in the ssoadm start-recording, ssoadm
get-recording-status, ssoadm stop-recording output and in the info.json file.",
          "title" : "Config export share password enabled",
          "type" : "boolean"
        }
```

```
      }
    },
    "debugLogs" : {
      "description" : "The debug level settings for the recording event.",
      "title" : "Debug level settings",
      "type" : "object",
      "properties" : {
        "debugLevel" : {
          "description" : "The debug level to set for the recording event.",
          "title" : "Debug level",
          "type" : "string",
          "enum" : [ "OFF", "ERROR", "WARNING", "MESSAGE", "ON" ]
        },
        "autoStop" : {
          "description" : "Used to specify an event that automatically ends a recording period. For
time-based termination, specify a time object; for termination based on uncompressed file size,
specify a fileSize object. If you specify both time and fileSize objects, the event that occurs first
causes recording to stop.",
          "title" : "Auto stop configuration",
          "type" : "object",
          "properties" : {
            "time" : {
              "description" : "Auto stop time based settings.",
              "title" : "Auto stop time configuration",
              "type" : "object",
              "properties" : {
                "timeUnit" : {
                  "description" : "The time unit that the auto stop time will be measured in, e.g.
MINUTES.",
                  "title" : "Auto stop time unit",
                  "type" : "string",
                  "enum" : [ "DAYS", "HOURS", "MINUTES", "SECONDS", "MILLISECONDS", "MICROSECONDS",
"NANOSECONDS" ]
                },
                "value" : {
                  "description" : "The time value for auto stop.",
                  "title" : "Auto stop time value",
                  "type" : "integer",
                  "format" : "int64"
                }
              }
            },
            "fileSize" : {
              "description" : "Configures a recording period to terminate after the aggregate size of
uncompressed debug logs has reached this size.",
              "title" : "Auto stop file size configuration",
              "type" : "object",
              "properties" : {
                "sizeUnit" : {
                  "description" : "The size unit that the auto stop will be measured in, e.g. GB.",
                  "title" : "Auto stop file size measurement unit",
                  "type" : "string",
                  "enum" : [ "GB", "MB", "KB", "B" ]
                },
                "value" : {
                  "description" : "The size value after which auto stop will occur",
                  "title" : "Auto stop file size value",
                  "type" : "integer",
                  "format" : "int64"
```

```
                }
              }
            }
          }
        }
      }
    },
    "zipEnable" : {
      "description" : "Whether to compress the output directory into a zip file when recording has
 stopped.",
      "title" : "Zip enabled",
      "type" : "boolean"
    }
  }
}
```

status

Returns status of recording.

Usage:

```
am> action Records --realm Realm --actionName status
```

stop

Stops recording.

Usage:

```
am> action Records --realm Realm --actionName stop
```

RecoveryCodeCollectorDecision

Realm Operations

Resource path: `/realm-config/authentication/authenticationtrees/nodes/RecoveryCodeCollectorDecisionNode`

Resource version: `1.0`

create

Usage:

```
am> create RecoveryCodeCollectorDecision --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "recoveryCodeType" : {
      "title" : "Recovery Code Type",
      "description" : "Determines which type of recovery codes are going to be validated for the
 user.",
      "propertyOrder" : 100,
      "type" : "string",
      "exampleValue" : ""
    }
  },
  "required" : [ "recoveryCodeType" ]
}
```

delete

Usage:

```
am> delete RecoveryCodeCollectorDecision --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action RecoveryCodeCollectorDecision --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action RecoveryCodeCollectorDecision --realm Realm --actionName getCreatableTypes
```

listOutcomes

List the available outcomes for the node type.

Usage:

```
am> action RecoveryCodeCollectorDecision --realm Realm --body body --actionName listOutcomes
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "title" : "Some configuration of the node. This does not need to be complete against the
 configuration schema."
}
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action RecoveryCodeCollectorDecision --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query RecoveryCodeCollectorDecision --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read RecoveryCodeCollectorDecision --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update RecoveryCodeCollectorDecision --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "recoveryCodeType" : {
      "title" : "Recovery Code Type",
      "description" : "Determines which type of recovery codes are going to be validated for the
 user.",
      "propertyOrder" : 100,
      "type" : "string",
      "exampleValue" : ""
    }
  },
  "required" : [ "recoveryCodeType" ]
}
```

RecoveryCodeDisplayNode

Realm Operations

Resource path: `/realm-config/authentication/authenticationtrees/nodes/RecoveryCodeDisplayNode`

Resource version: `1.0`

create

Usage:

```
am> create RecoveryCodeDisplayNode --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "required" : [ ]
}
```

delete

Usage:

```
am> delete RecoveryCodeDisplayNode --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action RecoveryCodeDisplayNode --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action RecoveryCodeDisplayNode --realm Realm --actionName getCreatableTypes
```

listOutcomes

List the available outcomes for the node type.

Usage:

```
am> action RecoveryCodeDisplayNode --realm Realm --body body --actionName listOutcomes
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "title" : "Some configuration of the node. This does not need to be complete against the
 configuration schema."
}
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action RecoveryCodeDisplayNode --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query RecoveryCodeDisplayNode --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read RecoveryCodeDisplayNode --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update RecoveryCodeDisplayNode --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "required" : [ ]
}
```

RegisterLogoutWebhook

Realm Operations

Resource path: `/realm-config/authentication/authenticationtrees/nodes/RegisterLogoutWebhookNode`

Resource version: `1.0`

create

Usage:

```
am> create RegisterLogoutWebhook --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "webhookName" : {
      "title" : "Webhook Name",
      "description" : "The name of the webhook stored using the webhook service.",
      "propertyOrder" : 100,
      "type" : "string",
      "exampleValue" : ""
    }
  },
  "required" : [ "webhookName" ]
}
```

delete

Usage:

```
am> delete RegisterLogoutWebhook --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action RegisterLogoutWebhook --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action RegisterLogoutWebhook --realm Realm --actionName getCreatableTypes
```

listOutcomes

List the available outcomes for the node type.

Usage:

```
am> action RegisterLogoutWebhook --realm Realm --body body --actionName listOutcomes
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "title" : "Some configuration of the node. This does not need to be complete against the
 configuration schema."
}
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action RegisterLogoutWebhook --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query RegisterLogoutWebhook --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read RegisterLogoutWebhook --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update RegisterLogoutWebhook --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "webhookName" : {
      "title" : "Webhook Name",
      "description" : "The name of the webhook stored using the webhook service.",
      "propertyOrder" : 100,
      "type" : "string",
      "exampleValue" : ""
    }
  },
  "required" : [ "webhookName" ]
}
```

RegisterThing

Realm Operations

Resource path: `/realm-config/authentication/authenticationtrees/nodes/IotRegistrationNode`

Resource version: `1.0`

create

Usage:

```
am> create RegisterThing --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "createIdentity" : {
      "title" : "Create Identity",
      "description" : "Create a new identity for the thing if one does not exist already.",
      "propertyOrder" : 20,
      "type" : "boolean",
```

```
      "exampleValue" : ""
    },
    "allowAttributeOverwrite" : {
      "title" : "Overwrite Attributes",
      "description" : "Allow existing identity attributes to be overwritten when new claims are
 provided for the thing.",
      "propertyOrder" : 50,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "claimToAttributeMapping" : {
      "title" : "Claim to Attribute Mapping",
      "description" : "Map the verified claims to the thing's attributes. The value on the left is the
 name of the claim in the verified claims JWT. The value on the right is the name of the attribute in
 the data store.",
      "propertyOrder" : 40,
      "patternProperties" : {
        ".*" : {
          "type" : "string"
        }
      },
      "type" : "object",
      "exampleValue" : ""
    },
    "allowKeyRotation" : {
      "title" : "Rotate Confirmation Key",
      "description" : "Allow multiple confirmation keys to be registered for a thing.",
      "propertyOrder" : 30,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "verifySubject" : {
      "title" : "Verify Certificate Subject",
      "description" : "Verify that the subject provided in the JWT is the same as either the X.509
 certificate subject CN or UID.",
      "propertyOrder" : 10,
      "type" : "boolean",
      "exampleValue" : ""
    }
  },
  "required" : [ "allowKeyRotation", "allowAttributeOverwrite", "claimToAttributeMapping",
 "createIdentity", "verifySubject" ]
}
```

delete

Usage:

```
am> delete RegisterThing --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action RegisterThing --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action RegisterThing --realm Realm --actionName getCreatableTypes
```

listOutcomes

List the available outcomes for the node type.

Usage:

```
am> action RegisterThing --realm Realm --body body --actionName listOutcomes
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "title" : "Some configuration of the node. This does not need to be complete against the
 configuration schema."
}
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action RegisterThing --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query RegisterThing --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read RegisterThing --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update RegisterThing --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "createIdentity" : {
      "title" : "Create Identity",
      "description" : "Create a new identity for the thing if one does not exist already.",
      "propertyOrder" : 20,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "allowAttributeOverwrite" : {
      "title" : "Overwrite Attributes",
      "description" : "Allow existing identity attributes to be overwritten when new claims are
 provided for the thing.",
      "propertyOrder" : 50,
      "type" : "boolean",
      "exampleValue" : ""
    },
```

```
    "claimToAttributeMapping" : {
      "title" : "Claim to Attribute Mapping",
      "description" : "Map the verified claims to the thing's attributes. The value on the left is the
 name of the claim in the verified claims JWT. The value on the right is the name of the attribute in
 the data store.",
      "propertyOrder" : 40,
      "patternProperties" : {
        ".*" : {
          "type" : "string"
        }
      },
      "type" : "object",
      "exampleValue" : ""
    },
    "allowKeyRotation" : {
      "title" : "Rotate Confirmation Key",
      "description" : "Allow multiple confirmation keys to be registered for a thing.",
      "propertyOrder" : 30,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "verifySubject" : {
      "title" : "Verify Certificate Subject",
      "description" : "Verify that the subject provided in the JWT is the same as either the X.509
 certificate subject CN or UID.",
      "propertyOrder" : 10,
      "type" : "boolean",
      "exampleValue" : ""
    }
  },
  "required" : [ "allowKeyRotation", "allowAttributeOverwrite", "claimToAttributeMapping",
 "createIdentity", "verifySubject" ]
}
```

RemoteConsentAgent

Realm Operations

Agents handler that is responsible for managing agents

Resource path: `/realm-config/agents/RemoteConsentAgent`

Resource version: `1.0`

create

Usage:

```
am> create RemoteConsentAgent --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "remoteConsentResponseEncryptionAlgorithm" : {
      "title" : "Consent response encryption algorithm",
      "description" : "The encryption algorithm to be used by the provider when decrypting the remote
 consent response JWT received from the Remote Consent Service.",
      "propertyOrder" : 34500,
      "type" : "object",
      "exampleValue" : "",
      "properties" : {
        "inherited" : {
          "type" : "boolean",
          "required" : true
        },
        "value" : {
          "type" : "string",
          "required" : false
        }
      }
    },
    "jwkSet" : {
      "title" : "Json Web Key",
      "description" : "Raw JSON Web Key value containing the Remote Consent Service's public keys.",
      "propertyOrder" : 35100,
      "type" : "object",
      "exampleValue" : "",
      "properties" : {
        "inherited" : {
          "type" : "boolean",
          "required" : true
        },
        "value" : {
          "type" : "string",
          "required" : false
        }
      }
    },
    "jwksCacheTimeout" : {
      "title" : "JWKs URI content cache timeout in ms",
      "description" : "To avoid loading the JWKS URI content for every operation, the JWKS content is
 cached. This timeout defines the maximum amount of time the JWKS URI content can be cached before
 being refreshed.",
      "propertyOrder" : 34900,
      "type" : "object",
      "exampleValue" : "",
      "properties" : {
        "inherited" : {
          "type" : "boolean",
          "required" : true
        },
```

```
        "value" : {
          "type" : "integer",
          "required" : true
        }
      }
    },
    "jwksUri" : {
      "title" : "Json Web Key URI",
      "description" : "The URI containing the public keys of the Remote Consent Service secret. The
 public keys are in the Json Web Key (jwk) format.",
      "propertyOrder" : 34800,
      "type" : "object",
      "exampleValue" : "",
      "properties" : {
        "inherited" : {
          "type" : "boolean",
          "required" : true
        },
        "value" : {
          "type" : "string",
          "required" : true
        }
      }
    },
    "jwkStoreCacheMissCacheTime" : {
      "title" : "JWKs URI content cache miss cache time",
      "description" : "To avoid loading the JWKS URI content for every operation, especially when
 the kid is not in the jwks content already cached, the JWKS content will be cached for a minimum
 period of time. This cache miss cache time defines the minimum amount of time the JWKS URI content is
 cached.",
      "propertyOrder" : 35000,
      "type" : "object",
      "exampleValue" : "",
      "properties" : {
        "inherited" : {
          "type" : "boolean",
          "required" : true
        },
        "value" : {
          "type" : "integer",
          "required" : true
        }
      }
    },
    "remoteConsentResponseEncryptionMethod" : {
      "title" : "Consent response encryption method",
      "description" : "The encryption method to be used by the provider when decrypting the remote
 consent response JWT received from the Remote Consent Service.<br><br>AM supports the following token
 encryption algorithms: <ul><li><code>A128GCM</code>, <code>A192GCM</code>, and <code>A256GCM</code> -
 AES in Galois Counter Mode (GCM) authenticated encryption mode.</li><li><code>A128CBC-HS256</code>,
 <code>A192CBC-HS384</code>, and <code>A256CBC-HS512</code> - AES encryption in CBC mode, with HMAC-
SHA-2 for integrity.</li></ul>",
      "propertyOrder" : 34600,
      "type" : "object",
      "exampleValue" : "",
      "properties" : {
        "inherited" : {
          "type" : "boolean",
          "required" : true
```

```
       },
       "value" : {
         "type" : "string",
         "required" : true
       }
     }
   },
   "remoteConsentRequestEncryptionMethod" : {
     "title" : "Consent request Encryption Method",
     "description" : "Encryption method to be used when encrypting the consent request JWT.",
     "propertyOrder" : 34300,
     "type" : "object",
     "exampleValue" : "",
     "properties" : {
       "inherited" : {
         "type" : "boolean",
         "required" : true
       },
       "value" : {
         "type" : "string",
         "required" : true
       }
     }
   },
   "requestTimeLimit" : {
     "title" : "Consent Request Time Limit",
     "description" : "The amount of seconds for which the consent request JWT sent to the Remote
Consent Service should be considered valid.",
     "propertyOrder" : 35200,
     "type" : "object",
     "exampleValue" : "",
     "properties" : {
       "inherited" : {
         "type" : "boolean",
         "required" : true
       },
       "value" : {
         "type" : "integer",
         "required" : false
       }
     }
   },
   "agentgroup" : {
     "title" : "Group",
     "description" : "Add the agent to a group to allow inheritance of property values from the
group. <br>Changing the group will update inherited property values. <br>Inherited property values
are copied to the agent.",
     "propertyOrder" : 50,
     "required" : false,
     "type" : "string",
     "exampleValue" : ""
   },
   "remoteConsentRequestEncryptionAlgorithm" : {
     "title" : "Consent request Encryption Algorithm",
     "description" : "Encryption algorithm to be used when encrypting the consent request JWT.",
     "propertyOrder" : 34200,
     "type" : "object",
     "exampleValue" : "",
     "properties" : {
```

```
        "inherited" : {
          "type" : "boolean",
          "required" : true
        },
        "value" : {
          "type" : "string",
          "required" : true
        }
      }
    },
    "remoteConsentRequestSigningAlgorithm" : {
      "title" : "Consent request Signing Algorithm",
      "description" : "Signing algorithm to be used when signing the consent request JWT.",
      "propertyOrder" : 34500,
      "type" : "object",
      "exampleValue" : "",
      "properties" : {
        "inherited" : {
          "type" : "boolean",
          "required" : true
        },
        "value" : {
          "type" : "string",
          "required" : true
        }
      }
    },
    "remoteConsentRedirectUrl" : {
      "title" : "Redirect URL",
      "description" : "The Remote Consent Service's URL to which the authorization server should
redirect the user in order to obtain their consent.",
      "propertyOrder" : 34000,
      "type" : "object",
      "exampleValue" : "",
      "properties" : {
        "inherited" : {
          "type" : "boolean",
          "required" : true
        },
        "value" : {
          "type" : "string",
          "required" : false
        }
      }
    },
    "remoteConsentResponseSigningAlg" : {
      "title" : "Consent response signing algorithm",
      "description" : "The signing algorithm to be used by the provider when verifying the signature
of the consent response JWT received from the Remote Consent Service.",
      "propertyOrder" : 34400,
      "type" : "object",
      "exampleValue" : "",
      "properties" : {
        "inherited" : {
          "type" : "boolean",
          "required" : true
        },
        "value" : {
          "type" : "string",
```

```
          "required" : false
        }
      }
    },
    "publicKeyLocation" : {
      "title" : "Public key selector",
      "description" : "",
      "propertyOrder" : 34700,
      "type" : "object",
      "exampleValue" : "",
      "properties" : {
        "inherited" : {
          "type" : "boolean",
          "required" : true
        },
        "value" : {
          "type" : "string",
          "required" : true
        }
      }
    },
    "userpassword" : {
      "title" : "Remote Consent Service secret",
      "description" : "Used when the Remote Consent Service authenticates to AM.",
      "propertyOrder" : 33000,
      "required" : true,
      "type" : "string",
      "format" : "password",
      "exampleValue" : ""
    },
    "remoteConsentRequestEncryptionEnabled" : {
      "title" : "Enable consent request Encryption",
      "description" : "Enables encryption of the consent request JWT.",
      "propertyOrder" : 34100,
      "type" : "object",
      "exampleValue" : "",
      "properties" : {
        "inherited" : {
          "type" : "boolean",
          "required" : true
        },
        "value" : {
          "type" : "boolean",
          "required" : true
        }
      }
    }
  }
}
```

delete

Usage:

```
am> delete RemoteConsentAgent --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action RemoteConsentAgent --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action RemoteConsentAgent --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action RemoteConsentAgent --realm Realm --actionName nextdescendents
```

query

Querying the agents of a specific type

Usage:

```
am> query RemoteConsentAgent --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read RemoteConsentAgent --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update RemoteConsentAgent --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "remoteConsentResponseEncryptionAlgorithm" : {
      "title" : "Consent response encryption algorithm",
      "description" : "The encryption algorithm to be used by the provider when decrypting the remote
 consent response JWT received from the Remote Consent Service.",
      "propertyOrder" : 34500,
      "type" : "object",
      "exampleValue" : "",
      "properties" : {
        "inherited" : {
          "type" : "boolean",
          "required" : true
        },
        "value" : {
          "type" : "string",
          "required" : false
        }
      }
    },
    "jwkSet" : {
      "title" : "Json Web Key",
      "description" : "Raw JSON Web Key value containing the Remote Consent Service's public keys.",
      "propertyOrder" : 35100,
      "type" : "object",
      "exampleValue" : "",
      "properties" : {
        "inherited" : {
          "type" : "boolean",
          "required" : true
        },
        "value" : {
          "type" : "string",
```

```
          "required" : false
        }
      }
    },
    "jwksCacheTimeout" : {
      "title" : "JWKs URI content cache timeout in ms",
      "description" : "To avoid loading the JWKS URI content for every operation, the JWKS content is
cached. This timeout defines the maximum amount of time the JWKS URI content can be cached before
being refreshed.",
      "propertyOrder" : 34900,
      "type" : "object",
      "exampleValue" : "",
      "properties" : {
        "inherited" : {
          "type" : "boolean",
          "required" : true
        },
        "value" : {
          "type" : "integer",
          "required" : true
        }
      }
    },
    "jwksUri" : {
      "title" : "Json Web Key URI",
      "description" : "The URI containing the public keys of the Remote Consent Service secret. The
public keys are in the Json Web Key (jwk) format.",
      "propertyOrder" : 34800,
      "type" : "object",
      "exampleValue" : "",
      "properties" : {
        "inherited" : {
          "type" : "boolean",
          "required" : true
        },
        "value" : {
          "type" : "string",
          "required" : true
        }
      }
    },
    "jwkStoreCacheMissCacheTime" : {
      "title" : "JWKs URI content cache miss cache time",
      "description" : "To avoid loading the JWKS URI content for every operation, especially when
the kid is not in the jwks content already cached, the JWKS content will be cached for a minimum
period of time. This cache miss cache time defines the minimum amount of time the JWKS URI content is
cached.",
      "propertyOrder" : 35000,
      "type" : "object",
      "exampleValue" : "",
      "properties" : {
        "inherited" : {
          "type" : "boolean",
          "required" : true
        },
        "value" : {
          "type" : "integer",
          "required" : true
        }
```

```
      }
    },
    "remoteConsentResponseEncryptionMethod" : {
      "title" : "Consent response encryption method",
      "description" : "The encryption method to be used by the provider when decrypting the remote
 consent response JWT received from the Remote Consent Service.<br><br>AM supports the following token
 encryption algorithms: <ul><li><code>A128GCM</code>, <code>A192GCM</code>, and <code>A256GCM</code> -
 AES in Galois Counter Mode (GCM) authenticated encryption mode.</li><li><code>A128CBC-HS256</code>,
 <code>A192CBC-HS384</code>, and <code>A256CBC-HS512</code> - AES encryption in CBC mode, with HMAC-
SHA-2 for integrity.</li></ul>",
      "propertyOrder" : 34600,
      "type" : "object",
      "exampleValue" : "",
      "properties" : {
        "inherited" : {
          "type" : "boolean",
          "required" : true
        },
        "value" : {
          "type" : "string",
          "required" : true
        }
      }
    },
    "remoteConsentRequestEncryptionMethod" : {
      "title" : "Consent request Encryption Method",
      "description" : "Encryption method to be used when encrypting the consent request JWT.",
      "propertyOrder" : 34300,
      "type" : "object",
      "exampleValue" : "",
      "properties" : {
        "inherited" : {
          "type" : "boolean",
          "required" : true
        },
        "value" : {
          "type" : "string",
          "required" : true
        }
      }
    },
    "requestTimeLimit" : {
      "title" : "Consent Request Time Limit",
      "description" : "The amount of seconds for which the consent request JWT sent to the Remote
 Consent Service should be considered valid.",
      "propertyOrder" : 35200,
      "type" : "object",
      "exampleValue" : "",
      "properties" : {
        "inherited" : {
          "type" : "boolean",
          "required" : true
        },
        "value" : {
          "type" : "integer",
          "required" : false
        }
      }
    },
```

```
    "agentgroup" : {
      "title" : "Group",
      "description" : "Add the agent to a group to allow inheritance of property values from the
group. <br>Changing the group will update inherited property values. <br>Inherited property values
are copied to the agent.",
      "propertyOrder" : 50,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
    },
    "remoteConsentRequestEncryptionAlgorithm" : {
      "title" : "Consent request Encryption Algorithm",
      "description" : "Encryption algorithm to be used when encrypting the consent request JWT.",
      "propertyOrder" : 34200,
      "type" : "object",
      "exampleValue" : "",
      "properties" : {
        "inherited" : {
          "type" : "boolean",
          "required" : true
        },
        "value" : {
          "type" : "string",
          "required" : true
        }
      }
    },
    "remoteConsentRequestSigningAlgorithm" : {
      "title" : "Consent request Signing Algorithm",
      "description" : "Signing algorithm to be used when signing the consent request JWT.",
      "propertyOrder" : 34500,
      "type" : "object",
      "exampleValue" : "",
      "properties" : {
        "inherited" : {
          "type" : "boolean",
          "required" : true
        },
        "value" : {
          "type" : "string",
          "required" : true
        }
      }
    },
    "remoteConsentRedirectUrl" : {
      "title" : "Redirect URL",
      "description" : "The Remote Consent Service's URL to which the authorization server should
redirect the user in order to obtain their consent.",
      "propertyOrder" : 34000,
      "type" : "object",
      "exampleValue" : "",
      "properties" : {
        "inherited" : {
          "type" : "boolean",
          "required" : true
        },
        "value" : {
          "type" : "string",
          "required" : false
```

```
        }
      }
    },
    "remoteConsentResponseSigningAlg" : {
      "title" : "Consent response signing algorithm",
      "description" : "The signing algorithm to be used by the provider when verifying the signature
of the consent response JWT received from the Remote Consent Service.",
      "propertyOrder" : 34400,
      "type" : "object",
      "exampleValue" : "",
      "properties" : {
        "inherited" : {
          "type" : "boolean",
          "required" : true
        },
        "value" : {
          "type" : "string",
          "required" : false
        }
      }
    },
    "publicKeyLocation" : {
      "title" : "Public key selector",
      "description" : "",
      "propertyOrder" : 34700,
      "type" : "object",
      "exampleValue" : "",
      "properties" : {
        "inherited" : {
          "type" : "boolean",
          "required" : true
        },
        "value" : {
          "type" : "string",
          "required" : true
        }
      }
    },
    "userpassword" : {
      "title" : "Remote Consent Service secret",
      "description" : "Used when the Remote Consent Service authenticates to AM.",
      "propertyOrder" : 33000,
      "required" : true,
      "type" : "string",
      "format" : "password",
      "exampleValue" : ""
    },
    "remoteConsentRequestEncryptionEnabled" : {
      "title" : "Enable consent request Encryption",
      "description" : "Enables encryption of the consent request JWT.",
      "propertyOrder" : 34100,
      "type" : "object",
      "exampleValue" : "",
      "properties" : {
        "inherited" : {
          "type" : "boolean",
          "required" : true
        },
        "value" : {
```

```
          "type" : "boolean",
          "required" : true
        }
      }
    }
  }
}
```

RemoteConsentService

Realm Operations

Resource path: `/realm-config/services/RemoteConsentService`

Resource version: `1.0`

create

Usage:

```
am> create RemoteConsentService --realm Realm --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "consentResponseTimeLimit" : {
      "title" : "Consent Response Time Limit (in minutes)",
      "description" : "The time limit set on the consent response JWT before it expires, in minutes.",
      "propertyOrder" : 700,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "clientId" : {
      "title" : "Client Name",
      "description" : "The name used to identify this OAuth 2.0 remote consent service when
 referencedin other services.",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "encryptionKeyAlias" : {
      "title" : "Encryption Key Alias",
      "description" : "The alias of the key in the default keystore to use for encryption.",
```

```
      "propertyOrder" : 300,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "signingKeyAlias" : {
      "title" : "Signing Key Alias",
      "description" : "The alias of the key in the default keystore to use for signing.",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "jwksUriAS" : {
      "title" : "Authorization Server jwk_uri",
      "description" : "The jwk_uri for retrieving the authorization server signing and encryption
 keys.",
      "propertyOrder" : 400,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "jwkStoreCacheMissCacheTime" : {
      "title" : "JWK Store Cache Miss Cache Time (in minutes)",
      "description" : "The length of time a cache miss is cached, in minutes.",
      "propertyOrder" : 600,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "jwkStoreCacheTimeout" : {
      "title" : "JWK Store Cache Timeout (in minutes)",
      "description" : "The cache timeout for the JWK store of the authorization server, in minutes.",
      "propertyOrder" : 500,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    }
  }
}
```


delete

Usage:

```
am> delete RemoteConsentService --realm Realm
```

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action RemoteConsentService --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action RemoteConsentService --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action RemoteConsentService --realm Realm --actionName nextdescendents
```

read

Usage:

```
am> read RemoteConsentService --realm Realm
```

update

Usage:

```
am> update RemoteConsentService --realm Realm --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "consentResponseTimeLimit" : {
      "title" : "Consent Response Time Limit (in minutes)",
      "description" : "The time limit set on the consent response JWT before it expires, in minutes.",
      "propertyOrder" : 700,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "clientId" : {
      "title" : "Client Name",
      "description" : "The name used to identify this OAuth 2.0 remote consent service when
 referencedin other services.",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
```

```
    },
    "encryptionKeyAlias" : {
      "title" : "Encryption Key Alias",
      "description" : "The alias of the key in the default keystore to use for encryption.",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "signingKeyAlias" : {
      "title" : "Signing Key Alias",
      "description" : "The alias of the key in the default keystore to use for signing.",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "jwksUriAS" : {
      "title" : "Authorization Server jwk_uri",
      "description" : "The jwk_uri for retrieving the authorization server signing and encryption
 keys.",
      "propertyOrder" : 400,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "jwkStoreCacheMissCacheTime" : {
      "title" : "JWK Store Cache Miss Cache Time (in minutes)",
      "description" : "The length of time a cache miss is cached, in minutes.",
      "propertyOrder" : 600,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "jwkStoreCacheTimeout" : {
      "title" : "JWK Store Cache Timeout (in minutes)",
      "description" : "The cache timeout for the JWK store of the authorization server, in minutes.",
      "propertyOrder" : 500,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    }
  }
}
```

Global Operations

Resource path: `/global-config/services/RemoteConsentService`

Resource version: `1.0`

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action RemoteConsentService --global --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action RemoteConsentService --global --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action RemoteConsentService --global --actionName nextdescendents
```

read

Usage:

```
am> read RemoteConsentService --global
```

update

Usage:

```
am> update RemoteConsentService --global --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "defaults" : {
      "properties" : {
        "clientId" : {
          "title" : "Client Name",
          "description" : "The name used to identify this OAuth 2.0 remote consent service when
 referencedin other services.",
          "propertyOrder" : 100,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
```

```
        "consentResponseTimeLimit" : {
          "title" : "Consent Response Time Limit (in minutes)",
          "description" : "The time limit set on the consent response JWT before it expires, in
 minutes.",
          "propertyOrder" : 700,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "jwkStoreCacheTimeout" : {
          "title" : "JWK Store Cache Timeout (in minutes)",
          "description" : "The cache timeout for the JWK store of the authorization server, in
 minutes.",
          "propertyOrder" : 500,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "encryptionKeyAlias" : {
          "title" : "Encryption Key Alias",
          "description" : "The alias of the key in the default keystore to use for encryption.",
          "propertyOrder" : 300,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "jwkStoreCacheMissCacheTime" : {
          "title" : "JWK Store Cache Miss Cache Time (in minutes)",
          "description" : "The length of time a cache miss is cached, in minutes.",
          "propertyOrder" : 600,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "signingKeyAlias" : {
          "title" : "Signing Key Alias",
          "description" : "The alias of the key in the default keystore to use for signing.",
          "propertyOrder" : 200,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "jwksUriAS" : {
          "title" : "Authorization Server jwk_uri",
          "description" : "The jwk_uri for retrieving the authorization server signing and encryption
 keys.",
          "propertyOrder" : 400,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      },
      "type" : "object",
      "title" : "Realm Defaults"
    }
  }
}
```

RemoteSaml2EntityProvider

Realm Operations

Allows the management of remote SAML2 entity providers.

Resource path: `/realm-config/saml2/remote`

Resource version: `1.0`

delete

Removes the SAML2 entity provider from the configuration including all of its associated roles.

Usage:

```
am> delete RemoteSaml2EntityProvider --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

importEntity

Import the standard metadata of a remote entity provider.

Usage:

```
am> action RemoteSaml2EntityProvider --realm Realm --body body --actionName importEntity
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "$schema" : "http://json-schema.org/draft-04/schema#",
  "description" : "The JSON schema for importEntity action requests.",
  "type" : "object",
  "title" : "Import remote entity provider request",
  "properties" : {
    "standardMetadata" : {
      "type" : "string",
      "title" : "Standard Metadata",
      "description" : "The standard SAML metadata for the remote entity provider. The value should be
 Base64url encoded."
    }
  },
  "required" : [ "standardMetadata" ]
}
```

read

Returns the roles of the SAML2 entity provider.

Usage:

```
am> read RemoteSaml2EntityProvider --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Updates details of the SAML2 entity provider role.

Usage:

```
am> update RemoteSaml2EntityProvider --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "$schema" : "http://json-schema.org/draft-07/schema#",
  "ignoredProperties" : [ "_id", "_rev" ],
  "description" : "This schema describes a remote SAML2 entity provider.",
  "title" : "SAML2 Remote Entity Provider",
  "type" : "object",
  "properties" : {
    "entityId" : {
      "type" : "string"
    },
    "identityProvider" : {
      "title" : "Remote Identity Provider",
      "description" : "This schema describes a SAML2 remote identity provider.",
      "type" : "object",
      "traverseObject" : true,
      "properties" : {
        "assertionContent" : {
          "propertyOrder" : 0,
          "traverseObject" : true,
          "title" : "Assertion Content",
          "type" : "object",
          "properties" : {
            "signingAndEncryption" : {
              "traverseObject" : true,
              "title" : "Signing And Encryption",
```

```
              "type" : "object",
              "properties" : {
                "requestResponseSigning" : {
                  "traverseObject" : true,
                  "title" : "Request/Response Signing",
                  "description" : "Select the checkbox for each request/response that should be
signed",
                  "type" : "object",
                  "properties" : {
                    "authenticationRequest" : {
                      "attributePath" : {
                        "value" : "/wantAuthnRequestsSigned"
                      },
                      "title" : "Authentication Request",
                      "type" : "boolean"
                    },
                    "artifactResolve" : {
                      "attributeKey" : "wantArtifactResolveSigned",
                      "title" : "Artifact Resolve",
                      "type" : "boolean"
                    },
                    "logoutRequest" : {
                      "attributeKey" : "wantLogoutRequestSigned",
                      "title" : "Logout Request",
                      "type" : "boolean"
                    },
                    "logoutResponse" : {
                      "attributeKey" : "wantLogoutResponseSigned",
                      "title" : "Logout Response",
                      "type" : "boolean"
                    },
                    "manageNameIdRequest" : {
                      "attributeKey" : "wantMNIRequestSigned",
                      "title" : "Manage NameID Request",
                      "type" : "boolean"
                    },
                    "manageNameIdResponse" : {
                      "attributeKey" : "wantMNIResponseSigned",
                      "title" : "Manage NameID Response",
                      "type" : "boolean"
                    }
                  },
                  "required" : [ "authenticationRequest", "artifactResolve", "logoutRequest",
"logoutResponse", "manageNameIdRequest", "manageNameIdResponse" ]
                },
                "encryption" : {
                  "traverseObject" : true,
                  "title" : "Encryption",
                  "type" : "object",
                  "properties" : {
                    "nameIdEncryption" : {
                      "attributeKey" : "wantNameIDEncrypted",
                      "title" : "NameID Encryption",
                      "type" : "boolean"
                    }
                  },
                  "required" : [ "nameIdEncryption" ]
                }
              }
```

```
            },
            "nameIdFormat" : {
              "traverseObject" : true,
              "title" : "NameID Format",
              "type" : "object",
              "properties" : {
                "nameIdFormatList" : {
                  "description" : "List of NameID formats the requestor will use to contact. Order
 listed shows the order of preference",
                  "title" : "NameID Format List",
                  "attributePath" : {
                    "value" : "/nameIDFormat"
                  },
                  "type" : "array",
                  "items" : {
                    "type" : "string"
                  },
                  "default" : [ "urn:oasis:names:tc:SAML:2.0:nameid-format:persistent",
 "urn:oasis:names:tc:SAML:2.0:nameid-format:transient", "urn:oasis:names:tc:SAML:1.1:nameid-
format:emailAddress", "urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified",
 "urn:oasis:names:tc:SAML:1.1:nameid-format:WindowsDomainQualifiedName",
 "urn:oasis:names:tc:SAML:2.0:nameid-format:kerberos", "urn:oasis:names:tc:SAML:1.1:nameid-
format:X509SubjectName" ]
                }
              }
            },
            "basicAuthentication" : {
              "traverseObject" : true,
              "description" : "Configure basic authentication setting for Soap based binding",
              "title" : "Basic Authentication",
              "type" : "object",
              "properties" : {
                "enabled" : {
                  "attributeKey" : "basicAuthOn",
                  "title" : "Enabled",
                  "type" : "boolean",
                  "default" : false
                },
                "userName" : {
                  "attributeKey" : "basicAuthUser",
                  "title" : "User Name",
                  "type" : "string"
                },
                "password" : {
                  "title" : "Password",
                  "attributeKey" : {
                    "value" : "basicAuthPassword",
                    "mapper" : "org.forgerock.openam.federation.rest.schema.mappers.PasswordMapper"
                  },
                  "type" : "string",
                  "format" : "password"
                }
              }
            }
          }
        },
        "services" : {
          "propertyOrder" : 1,
          "traverseObject" : true,
```

```
          "title" : "Services",
          "type" : "object",
          "properties" : {
            "serviceAttributes" : {
              "type" : "object",
              "title" : "IDP Service Attributes",
              "traverseObject" : true,
              "properties" : {
                "artifactResolutionService" : {
                  "title" : "Artifact Resolution Service",
                  "type" : "array",
                  "attributePath" : {
                    "value" : "artifactResolutionService",
                    "mapper" :
"org.forgerock.openam.federation.rest.schema.mappers.IndexedEndpointMapper"
                  },
                  "items" : {
                    "type" : "object",
                    "properties" : {
                      "binding" : {
                        "title" : "Binding",
                        "anyOf" : [ {
                          "title" : "Predefined Binding",
                          "type" : "string",
                          "enum" : [ "urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect",
"urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST", "urn:oasis:names:tc:SAML:2.0:bindings:SOAP",
"urn:oasis:names:tc:SAML:2.0:bindings:PAOS" ],
                          "enumNames" : [ "HTTP-REDIRECT", "HTTP-POST", "SOAP", "PAOS" ]
                        }, {
                          "title" : "Custom Binding",
                          "type" : "string"
                        } ]
                      },
                      "location" : {
                        "title" : "Location",
                        "type" : "string"
                      },
                      "responseLocation" : {
                        "title" : "Response Location",
                        "type" : "string"
                      }
                    },
                    "required" : [ "location" ]
                  }
                },
                "singleLogoutService" : {
                  "title" : "Single Logout Service",
                  "type" : "array",
                  "attributePath" : {
                    "value" : "singleLogoutService",
                    "mapper" : "org.forgerock.openam.federation.rest.schema.mappers.EndpointMapper"
                  },
                  "items" : {
                    "type" : "object",
                    "properties" : {
                      "binding" : {
                        "title" : "Binding",
                        "anyOf" : [ {
                          "title" : "Predefined Binding",
```

```
                        "type" : "string",
                        "enum" : [ "urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect",
"urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST", "urn:oasis:names:tc:SAML:2.0:bindings:SOAP",
"urn:oasis:names:tc:SAML:2.0:bindings:PAOS" ],
                        "enumNames" : [ "HTTP-REDIRECT", "HTTP-POST", "SOAP", "PAOS" ]
                      }, {
                        "title" : "Custom Binding",
                        "type" : "string"
                      } ]
                    },
                    "location" : {
                      "title" : "Location",
                      "type" : "string"
                    },
                    "responseLocation" : {
                      "title" : "Response Location",
                      "type" : "string"
                    }
                  },
                  "required" : [ "location" ]
                }
              },
              "nameIdService" : {
                "title" : "Manage NameID Service",
                "type" : "array",
                "attributePath" : {
                  "value" : "manageNameIDService",
                  "mapper" : "org.forgerock.openam.federation.rest.schema.mappers.EndpointMapper"
                },
                "items" : {
                  "type" : "object",
                  "properties" : {
                    "binding" : {
                      "title" : "Binding",
                      "anyOf" : [ {
                        "title" : "Predefined Binding",
                        "type" : "string",
                        "enum" : [ "urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect",
"urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST", "urn:oasis:names:tc:SAML:2.0:bindings:SOAP",
"urn:oasis:names:tc:SAML:2.0:bindings:PAOS" ],
                        "enumNames" : [ "HTTP-REDIRECT", "HTTP-POST", "SOAP", "PAOS" ]
                      }, {
                        "title" : "Custom Binding",
                        "type" : "string"
                      } ]
                    },
                    "location" : {
                      "title" : "Location",
                      "type" : "string"
                    },
                    "responseLocation" : {
                      "title" : "Response Location",
                      "type" : "string"
                    }
                  },
                  "required" : [ "location" ]
                }
              },
              "singleSignOnService" : {
```

```
                "title" : "Single SignOn Service",
                "type" : "array",
                "attributePath" : {
                  "value" : "singleSignOnService",
                  "mapper" : "org.forgerock.openam.federation.rest.schema.mappers.EndpointMapper"
                },
                "items" : {
                  "type" : "object",
                  "properties" : {
                    "binding" : {
                      "title" : "Binding",
                      "anyOf" : [ {
                        "title" : "Predefined Binding",
                        "type" : "string",
                        "enum" : [ "urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect",
"urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST", "urn:oasis:names:tc:SAML:2.0:bindings:SOAP",
"urn:oasis:names:tc:SAML:2.0:bindings:PAOS" ],
                        "enumNames" : [ "HTTP-REDIRECT", "HTTP-POST", "SOAP", "PAOS" ]
                      }, {
                        "title" : "Custom Binding",
                        "type" : "string"
                      } ]
                    },
                    "location" : {
                      "title" : "Location",
                      "type" : "string"
                    },
                    "responseLocation" : {
                      "title" : "Response Location",
                      "type" : "string"
                    }
                  },
                  "required" : [ "location" ]
                }
              }
            }
          },
          "nameIdMapping" : {
            "title" : "NameID Mapping",
            "type" : "array",
            "attributePath" : {
              "value" : "nameIDMappingService",
              "mapper" : "org.forgerock.openam.federation.rest.schema.mappers.EndpointMapper"
            },
            "items" : {
              "type" : "object",
              "properties" : {
                "binding" : {
                  "title" : "Binding",
                  "anyOf" : [ {
                    "title" : "Predefined Binding",
                    "type" : "string",
                    "enum" : [ "urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect",
"urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST", "urn:oasis:names:tc:SAML:2.0:bindings:SOAP",
"urn:oasis:names:tc:SAML:2.0:bindings:PAOS" ],
                    "enumNames" : [ "HTTP-REDIRECT", "HTTP-POST", "SOAP", "PAOS" ]
                  }, {
                    "title" : "Custom Binding",
                    "type" : "string"
```

```
                  } ]
                },
                "location" : {
                  "title" : "Location",
                  "type" : "string"
                },
                "responseLocation" : {
                  "title" : "Response Location",
                  "type" : "string"
                }
              },
              "required" : [ "location" ]
            }
          }
        }
      }
    }
  },
  "serviceProvider" : {
    "title" : "Remote Service Provider",
    "description" : "This schema describes a SAML2 remote service provider.",
    "type" : "object",
    "traverseObject" : true,
    "properties" : {
      "assertionContent" : {
        "propertyOrder" : 0,
        "traverseObject" : true,
        "title" : "Assertion Content",
        "type" : "object",
        "properties" : {
          "signingAndEncryption" : {
            "traverseObject" : true,
            "title" : "Signing And Encryption",
            "type" : "object",
            "properties" : {
              "requestResponseSigning" : {
                "traverseObject" : true,
                "description" : "Select the checkbox for each request/response that should be
signed",
                "title" : "Request/Response Signing",
                "type" : "object",
                "properties" : {
                  "authenticationRequest" : {
                    "attributePath" : {
                      "value" : "/authnRequestsSigned"
                    },
                    "title" : "Authentication Requests Signed",
                    "type" : "boolean"
                  },
                  "assertion" : {
                    "attributePath" : "/wantAssertionsSigned",
                    "title" : "Assertions Signed",
                    "type" : "boolean"
                  },
                  "postResponse" : {
                    "attributeKey" : "wantPOSTResponseSigned",
                    "title" : "POST Response Signed",
                    "type" : "boolean"
                  },
```

```
                    "artifactResponse" : {
                      "attributeKey" : "wantArtifactResponseSigned",
                      "title" : "Artifact Response Signed",
                      "type" : "boolean"
                    },
                    "logoutRequest" : {
                      "attributeKey" : "wantLogoutRequestSigned",
                      "title" : "Logout Request Signed",
                      "type" : "boolean"
                    },
                    "logoutResponse" : {
                      "attributeKey" : "wantLogoutResponseSigned",
                      "title" : "Logout Response Signed",
                      "type" : "boolean"
                    },
                    "manageNameIdRequest" : {
                      "attributeKey" : "wantMNIRequestSigned",
                      "title" : "Manage NameID Request Signed",
                      "type" : "boolean"
                    },
                    "manageNameIdResponse" : {
                      "attributeKey" : "wantMNIResponseSigned",
                      "title" : "Manage NameID Response Signed",
                      "type" : "boolean"
                    }
                  }
                },
                "encryption" : {
                  "traverseObject" : true,
                  "title" : "Encryption",
                  "type" : "object",
                  "properties" : {
                    "attributeEncryption" : {
                      "attributeKey" : "wantAttributeEncrypted",
                      "title" : "Attribute Encryption",
                      "type" : "boolean"
                    },
                    "assertionEncryption" : {
                      "attributeKey" : "wantAssertionEncrypted",
                      "title" : "Assertion Encryption",
                      "type" : "boolean"
                    },
                    "nameIdEncryption" : {
                      "attributeKey" : "wantNameIDEncrypted",
                      "title" : "NameID Encryption",
                      "type" : "boolean"
                    }
                  }
                }
              }
            },
            "nameIdFormat" : {
              "traverseObject" : true,
              "title" : "NameID Format",
              "type" : "object",
              "properties" : {
                "nameIdFormatList" : {
                  "description" : "List of NameID formats the requestor will use to contact. Order
listed shows the order of preference",
```

```
                "title" : "NameID Format List",
                "attributePath" : {
                  "value" : "/nameIDFormat"
                },
                "type" : "array",
                "items" : {
                  "type" : "string"
                },
                "default" : [ "urn:oasis:names:tc:SAML:2.0:nameid-format:persistent",
 "urn:oasis:names:tc:SAML:2.0:nameid-format:transient", "urn:oasis:names:tc:SAML:1.1:nameid-
format:emailAddress", "urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified",
 "urn:oasis:names:tc:SAML:1.1:nameid-format:WindowsDomainQualifiedName",
 "urn:oasis:names:tc:SAML:2.0:nameid-format:kerberos", "urn:oasis:names:tc:SAML:1.1:nameid-
format:X509SubjectName" ]
              },
              "disableNameIdPersistence" : {
                "attributeKey" : "spDoNotWriteFederationInfo",
                "title" : "Disable NameID persistence",
                "description" : "Instructs the hosted IdP to not persist the NameID into the User
 Data Store even if the NameID Format is urn:oasis:names:tc:SAML:2.0:nameid-format:persistent in the
 Assertion.",
                "type" : "boolean"
              }
            }
          },
          "basicAuthentication" : {
            "traverseObject" : true,
            "description" : "Configure basic authentication setting for Soap based binding",
            "title" : "Basic Authentication",
            "type" : "object",
            "properties" : {
              "enabled" : {
                "attributeKey" : "basicAuthOn",
                "title" : "Enabled",
                "type" : "boolean",
                "default" : false
              },
              "userName" : {
                "attributeKey" : "basicAuthUser",
                "title" : "User Name",
                "type" : "string"
              },
              "password" : {
                "title" : "Password",
                "attributeKey" : {
                  "value" : "basicAuthPassword",
                  "mapper" : "org.forgerock.openam.federation.rest.schema.mappers.PasswordMapper"
                },
                "type" : "string",
                "format" : "password"
              }
            }
          }
        }
      },
      "assertionProcessing" : {
        "propertyOrder" : 1,
        "traverseObject" : true,
        "title" : "Assertion Processing",
```

```
          "type" : "object",
          "properties" : {
            "attributeMapper" : {
              "traverseObject" : true,
              "title" : "Attribute Mapper",
              "type" : "object",
              "properties" : {
                "attributeMap" : {
                  "title" : "Attribute Map",
                  "description" : "This mapping is the configuration used by the Attribue Mapper.
Mapping should be defined as SAML ATTRIBUTE NAME=PROFILE ATTRIBUTE NAME in assertion. Example:
EmailAddress=mail, Address=postaladdress.",
                  "type" : "array",
                  "attributeKey" : {
                    "value" : "attributeMap",
                    "mapper" :
"org.forgerock.openam.federation.rest.schema.mappers.AttributeMapMapper"
                  },
                  "items" : {
                    "type" : "object",
                    "properties" : {
                      "nameFormatUri" : {
                        "title" : "Name Format Uri",
                        "propertyOrder" : 0,
                        "type" : "string"
                      },
                      "samlAttribute" : {
                        "title" : "SAML Attribute",
                        "propertyOrder" : 1,
                        "type" : "string"
                      },
                      "localAttribute" : {
                        "title" : "Local Attribute",
                        "propertyOrder" : 2,
                        "type" : "string"
                      },
                      "binary" : {
                        "title" : "Binary",
                        "propertyOrder" : 3,
                        "type" : "boolean"
                      }
                    },
                    "required" : [ "samlAttribute", "localAttribute" ]
                  }
                }
              }
            },
            "responseArtifactMessageEncoding" : {
              "traverseObject" : true,
              "title" : "Artifact Message Encoding",
              "type" : "object",
              "properties" : {
                "encoding" : {
                  "attributeKey" : {
                    "value" : "responseArtifactMessageEncoding",
                    "mapper" :
"org.forgerock.openam.federation.rest.schema.mappers.MessageEncodingMapper"
                  },
                  "title" : "Artifact Message Encoding",
```

```
                "type" : "string",
                "enum" : [ "URI", "FORM" ],
                "default" : "URI"
              }
            }
          }
        }
      },
      "services" : {
        "propertyOrder" : 2,
        "traverseObject" : true,
        "title" : "Services",
        "type" : "object",
        "properties" : {
          "serviceAttributes" : {
            "traverseObject" : true,
            "title" : "SP Service Attributes",
            "type" : "object",
            "properties" : {
              "singleLogoutService" : {
                "title" : "Single Logout Service",
                "type" : "array",
                "attributePath" : {
                  "value" : "singleLogoutService",
                  "mapper" : "org.forgerock.openam.federation.rest.schema.mappers.EndpointMapper"
                },
                "items" : {
                  "type" : "object",
                  "properties" : {
                    "binding" : {
                      "title" : "Binding",
                      "anyOf" : [ {
                        "title" : "Predefined Binding",
                        "type" : "string",
                        "enum" : [ "urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect",
"urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST", "urn:oasis:names:tc:SAML:2.0:bindings:SOAP",
"urn:oasis:names:tc:SAML:2.0:bindings:PAOS" ],
                        "enumNames" : [ "HTTP-REDIRECT", "HTTP-POST", "SOAP", "PAOS" ]
                      }, {
                        "title" : "Custom Binding",
                        "type" : "string"
                      } ]
                    },
                    "location" : {
                      "title" : "Location",
                      "type" : "string"
                    },
                    "responseLocation" : {
                      "title" : "Response Location",
                      "type" : "string"
                    }
                  },
                  "required" : [ "location" ]
                },
                "post" : {
                  "type" : "object",
                  "properties" : {
                    "binding" : {
                      "title" : "Binding",
```

```
                        "anyOf" : [ {
                          "title" : "Predefined Binding",
                          "type" : "string",
                          "enum" : [ "urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect",
"urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST", "urn:oasis:names:tc:SAML:2.0:bindings:SOAP",
"urn:oasis:names:tc:SAML:2.0:bindings:PAOS" ],
                          "enumNames" : [ "HTTP-REDIRECT", "HTTP-POST", "SOAP", "PAOS" ]
                        }, {
                          "title" : "Custom Binding",
                          "type" : "string"
                        } ]
                      },
                      "location" : {
                        "title" : "Location",
                        "type" : "string"
                      },
                      "responseLocation" : {
                        "title" : "Response Location",
                        "type" : "string"
                      }
                    },
                    "required" : [ "location" ]
                  },
                  "soap" : {
                    "type" : "object",
                    "properties" : {
                      "location" : {
                        "type" : "string"
                      }
                    },
                    "required" : [ "location" ]
                  }
                },
                "nameIdService" : {
                  "title" : "Manage NameID Service",
                  "type" : "array",
                  "attributePath" : {
                    "value" : "manageNameIDService",
                    "mapper" : "org.forgerock.openam.federation.rest.schema.mappers.EndpointMapper"
                  },
                  "items" : {
                    "type" : "object",
                    "properties" : {
                      "binding" : {
                        "title" : "Binding",
                        "anyOf" : [ {
                          "title" : "Predefined Binding",
                          "type" : "string",
                          "enum" : [ "urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect",
"urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST", "urn:oasis:names:tc:SAML:2.0:bindings:SOAP",
"urn:oasis:names:tc:SAML:2.0:bindings:PAOS" ],
                          "enumNames" : [ "HTTP-REDIRECT", "HTTP-POST", "SOAP", "PAOS" ]
                        }, {
                          "title" : "Custom Binding",
                          "type" : "string"
                        } ]
                      },
                      "location" : {
                        "title" : "Location",
```

```
                      "type" : "string"
                    },
                    "responseLocation" : {
                      "title" : "Response Location",
                      "type" : "string"
                    }
                  },
                  "required" : [ "location" ]
                },
                "soap" : {
                  "type" : "object",
                  "properties" : {
                    "location" : {
                      "type" : "string"
                    }
                  },
                  "required" : [ "location" ]
                }
              },
              "assertionConsumerService" : {
                "attributePath" : {
                  "value" : "assertionConsumerService",
                  "mapper" :
"org.forgerock.openam.federation.rest.schema.mappers.ExtendedIndexedEndpointMapper"
                },
                "title" : "Assertion Consumer Service",
                "description" : "Location denotes the URL to accept the respective request type.
Index denotes the index of the URL in the standard metadata",
                "type" : "array",
                "items" : {
                  "type" : "object",
                  "properties" : {
                    "isDefault" : {
                      "type" : "boolean"
                    },
                    "binding" : {
                      "title" : "Binding",
                      "anyOf" : [ {
                        "title" : "Predefined Binding",
                        "type" : "string",
                        "enum" : [ "urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Artifact",
"urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST", "urn:oasis:names:tc:SAML:2.0:bindings:PAOS" ],
                        "enumNames" : [ "HTTP-Artifact", "HTTP-POST", "PAOS" ]
                      }, {
                        "title" : "Custom Binding",
                        "type" : "string"
                      } ]
                    },
                    "location" : {
                      "title" : "Location",
                      "type" : "string"
                    },
                    "index" : {
                      "type" : "integer"
                    }
                  }
                }
              }
            }
```

```
            }
          }
        },
        "advanced" : {
          "propertyOrder" : 3,
          "traverseObject" : true,
          "title" : "Advanced",
          "type" : "object",
          "properties" : {
            "skipEndpointValidationWhenSigned" : {
              "title" : "Skip Endpoint Validation For Signed Requests",
              "description" : "When enabled, AM will not attempt to verify the
AssertionConsumerServiceURL value provided in the SAML AuthnRequest. This SP MUST also be configured
to sign authentication requests",
              "type" : "boolean",
              "attributeKey" : "skipEndpointValidationWhenSigned"
            },
            "saeConfiguration" : {
              "traverseObject" : true,
              "title" : "SAE Configuration",
              "type" : "object",
              "properties" : {
                "spUrl" : {
                  "attributeKey" : "saeSPUrl",
                  "title" : "SP URL",
                  "description" : "URL endpoint on Service Provider that can handle SAE requests.
If this URL is empty (not configured), SAE single sign-on will not be enabled. Normal samlv2 single
sign-on response will be sent to SP",
                  "type" : "string"
                },
                "spLogoutUrl" : {
                  "attributeKey" : "saeSPLogoutUrl",
                  "title" : "SP Logout URL",
                  "description" : "URL endpoint on the Service Provider that can handle SAE global
logout requests",
                  "type" : "string"
                }
              }
            },
            "idpProxy" : {
              "traverseObject" : true,
              "title" : "IDP Proxy",
              "type" : "object",
              "properties" : {
                "enableIdpProxy" : {
                  "attributeKey" : "enableIDPProxy",
                  "title" : "IDP Proxy enabled",
                  "description" : "Enable IDP Proxy if not enabled",
                  "type" : "boolean"
                },
                "alwaysIdpProxy" : {
                  "attributeKey" : "alwaysIdpProxy",
                  "title" : "Proxy all requests",
                  "description" : "When this option is enabled, the IdP will proxy every single
authentication request no matter it contains the Scoping element or not.",
                  "type" : "boolean"
                },
                "useIntroductionForIdpProxy" : {
                  "attributeKey" : "useIntroductionForIDPProxy",
```

```
                  "title" : "Introduction enabled",
                  "type" : "boolean"
                },
                "useIDPFinder" : {
                  "attributeKey" : "useIDPFinder",
                  "title" : "Use IDP Finder",
                  "type" : "boolean"
                },
                "idpProxyCount" : {
                  "attributeKey" : "idpProxyCount",
                  "title" : "Proxy Count",
                  "description" : "Number of IDP proxies that the SP can have",
                  "type" : "integer",
                  "default" : 0
                },
                "idpProxyList" : {
                  "attributeKey" : "idpProxyList",
                  "description" : "A list of preferred IDPs that the SP would proxy to",
                  "title" : "IDP Proxy List",
                  "type" : "array",
                  "items" : {
                    "type" : "string"
                  }
                }
              }
            }
          }
        }
      }
    }
  },
  "required" : [ "entityId" ],
  "$id" : "https://www.forgerock.com/remoteSaml2EntityProvider.schema.json"
}
```

RemoveSessionProperties

Realm Operations

Resource path: `/realm-config/authentication/authenticationtrees/nodes/RemoveSessionPropertiesNode`

Resource version: `1.0`

create

Usage:

```
am> create RemoveSessionProperties --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "propertyNames" : {
      "title" : "Property Names",
      "description" : "The names of session properties to remove that may have been contributed by
 nodes that executedearlier in the tree. If the properties do not exist, no error will be thrown.
 Names are case sensitive.",
      "propertyOrder" : 100,
      "items" : {
        "type" : "string"
      },
      "minItems" : 1,
      "type" : "array",
      "exampleValue" : ""
    }
  },
  "required" : [ "propertyNames" ]
}
```

delete

Usage:

```
am> delete RemoveSessionProperties --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action RemoveSessionProperties --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action RemoveSessionProperties --realm Realm --actionName getCreatableTypes
```

listOutcomes

List the available outcomes for the node type.

Usage:

```
am> action RemoveSessionProperties --realm Realm --body body --actionName listOutcomes
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "title" : "Some configuration of the node. This does not need to be complete against the
 configuration schema."
}
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action RemoveSessionProperties --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query RemoveSessionProperties --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read RemoveSessionProperties --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update RemoveSessionProperties --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "propertyNames" : {
      "title" : "Property Names",
      "description" : "The names of session properties to remove that may have been contributed by
 nodes that executedearlier in the tree. If the properties do not exist, no error will be thrown.
 Names are case sensitive.",
      "propertyOrder" : 100,
      "items" : {
        "type" : "string"
      },
      "minItems" : 1,
      "type" : "array",
      "exampleValue" : ""
    }
  },
  "required" : [ "propertyNames" ]
}
```

RequiredAttributesPresent

Realm Operations

Resource path: `/realm-config/authentication/authenticationtrees/nodes/RequiredAttributesDecisionNode`

Resource version: `1.0`

create

Usage:

```
am> create RequiredAttributesPresent --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "identityResource" : {
      "title" : "Identity Resource",
      "description" : "The identity resource in IDM for which the required attributes list will be
 fetched. Must match identity resource of the current tree.",
      "propertyOrder" : 100,
      "type" : "string",
      "exampleValue" : ""
    }
  },
  "required" : [ "identityResource" ]
}
```

delete

Usage:

```
am> delete RequiredAttributesPresent --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action RequiredAttributesPresent --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action RequiredAttributesPresent --realm Realm --actionName getCreatableTypes
```

listOutcomes

List the available outcomes for the node type.

Usage:

```
am> action RequiredAttributesPresent --realm Realm --body body --actionName listOutcomes
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "title" : "Some configuration of the node. This does not need to be complete against the
 configuration schema."
}
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action RequiredAttributesPresent --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query RequiredAttributesPresent --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read RequiredAttributesPresent --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update RequiredAttributesPresent --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "identityResource" : {
      "title" : "Identity Resource",
      "description" : "The identity resource in IDM for which the required attributes list will be
 fetched. Must match identity resource of the current tree.",
      "propertyOrder" : 100,
      "type" : "string",
      "exampleValue" : ""
    }
  },
  "required" : [ "identityResource" ]
}
```

ResourceSets

Realm Operations

Resource set resource provider is responsible for managing Resource Sets belonging to a user. Available operations are update, query, read, revoke all action.

Resource path: `/users/{user}/oauth2/resources/sets`

Resource version: `1.0`

query

Query the collection of the user's Resource Set.

Usage:

```
am> query ResourceSets --realm Realm --filter filter --user user
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all. Fields that can be queried: [*]

--user

Resource set resource provider is responsible for managing Resource Sets belonging to a user. Available operations are update, query, read, revoke all action.

read

Read Resource Set from the collection by id.

Usage:

```
am> read ResourceSets --realm Realm --id id --user user
```

Parameters:

--id

The unique identifier for the resource.

--user

Resource set resource provider is responsible for managing Resource Sets belonging to a user. Available operations are update, query, read, revoke all action.

update

Update a Resource Set record.

Usage:

```
am> update ResourceSets --realm Realm --id id --body body --user user
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "$schema" : "http://json-schema.org/draft-04/schema#",
  "description" : "Describes the structure of the OpenAM representation of a user's OAuth Resource
 Set. For further  information see [insert link to the RSR standard], and documentation about UMA in
 OpenAM.",
  "type" : "object",
  "title" : "Resource Set resource schema",
  "properties" : {
    "scopes" : {
      "type" : "array",
      "title" : "Scopes",
      "description" : "List of Resource Set scopes.",
      "items" : {
        "type" : "string"
      }
    },
    "_id" : {
      "type" : "string",
      "title" : "Resource set id",
      "description" : "Unique identifier of the Resource Set."
    },
    "resourceServer" : {
      "type" : "string",
      "title" : "Resource server",
      "description" : "The resources server name."
    },
    "labels" : {
      "type" : "array",
      "title" : "Resource labels",
      "description" : "Labels of the resource.",
      "items" : {
        "type" : "string"
      }
    },
    "name" : {
      "type" : "string",
      "title" : "Resource name",
      "description" : "Name of the resource."
    },
    "icon_uri" : {
      "type" : "string",
      "title" : "Icon uri",
      "description" : "Resource icon uri."
    },
    "resourceOwnerId" : {
      "type" : "string",
      "title" : "Resource owner",
      "description" : "Name of the resource owner."
    },
    "type" : {
      "type" : "string",
      "title" : "Resource type",
      "description" : "Type of the resources."
    }
  }
```

```
}
```

--user

Resource set resource provider is responsible for managing Resource Sets belonging to a user. Available operations are update, query, read, revoke all action.

ResourceTypes

Realm Operations

The Resource Types resource is responsible for managing resource types, which define a template for the resources that Managing Policies policies apply to, and the actions associated with those resources. Available operations are Query, Read, Create, Update, Delete

Resource path: `/resourcetypes`

Resource version: `1.0`

create

Create new resource type

Usage:

```
am> create ResourceTypes --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "$schema" : "http://json-schema.org/draft-04/schema#",
  "description" : "Resource Types Resource schema",
  "type" : "object",
  "title" : "Resource Types Resource schema",
  "properties" : {
    "uuid" : {
      "title" : "UUID",
      "description" : "Unique identifier of the record",
      "type" : "string"
    },
    "name" : {
      "title" : "Name",
```

```
      "description" : "Resource type name",
      "type" : "string"
    },
    "description" : {
      "title" : "Description",
      "description" : "Resource type description",
      "type" : "string"
    },
    "patterns" : {
      "title" : "Patterns",
      "description" : "Resource type patterns",
      "type" : "array",
      "items" : {
        "type" : "string"
      }
    },
    "actions" : {
      "title" : "Actions",
      "description" : "Resource type actions",
      "type" : "object",
      "additionalProperties" : {
        "type" : "boolean"
      }
    },
    "createdBy" : {
      "title" : "Created by",
      "description" : "A string containing the universal identifier DN of the subject created the
 resource type",
      "type" : "string"
    },
    "creationDate" : {
      "title" : "Creation date",
      "description" : "An integer containing the creation date and time, in ISO 8601 format",
      "type" : "number"
    },
    "lastModifiedBy" : {
      "title" : "Last modifier",
      "description" : "A string containing the universal identifier DN of the subject that most
 recently updated the resource type. If the resource type has not been modified since it was created,
 this property will have the same value as createdBy",
      "type" : "string"
    },
    "lastModifiedDate" : {
      "title" : "Last modification date",
      "description" : "A string containing the last modified date and time, in ISO 8601 format. If the
 resource typ has not been modified since it was created, this property will have the same value as
 creationDate",
      "type" : "number"
    }
  }
}
```

delete

Delete resource type

Usage:

```
am> delete ResourceTypes --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

query

Query the collection of resource types

Usage:

```
am> query ResourceTypes --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all. Fields that can be queried: [*]

read

Read from the resource types collection by unique identifier

Usage:

```
am> read ResourceTypes --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Update an existing resource type

Usage:

```
am> update ResourceTypes --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "$schema" : "http://json-schema.org/draft-04/schema#",
  "description" : "Resource Types Resource schema",
  "type" : "object",
  "title" : "Resource Types Resource schema",
  "properties" : {
    "uuid" : {
      "title" : "UUID",
      "description" : "Unique identifier of the record",
      "type" : "string"
    },
    "name" : {
      "title" : "Name",
      "description" : "Resource type name",
      "type" : "string"
    },
    "description" : {
      "title" : "Description",
      "description" : "Resource type description",
      "type" : "string"
    },
    "patterns" : {
      "title" : "Patterns",
      "description" : "Resource type patterns",
      "type" : "array",
      "items" : {
        "type" : "string"
      }
    },
    "actions" : {
      "title" : "Actions",
      "description" : "Resource type actions",
      "type" : "object",
      "additionalProperties" : {
        "type" : "boolean"
      }
    },
    "createdBy" : {
      "title" : "Created by",
      "description" : "A string containing the universal identifier DN of the subject created the
 resource type",
      "type" : "string"
    },
    "creationDate" : {
      "title" : "Creation date",
      "description" : "An integer containing the creation date and time, in ISO 8601 format",
      "type" : "number"
    },
    "lastModifiedBy" : {
      "title" : "Last modifier",
      "description" : "A string containing the universal identifier DN of the subject that most
 recently updated the resource type. If the resource type has not been modified since it was created,
 this property will have the same value as createdBy",
      "type" : "string"
    },
```

```
    "lastModifiedDate" : {
      "title" : "Last modification date",
      "description" : "A string containing the last modified date and time, in ISO 8601 format. If the
 resource typ has not been modified since it was created, this property will have the same value as
 creationDate",
      "type" : "number"
    }
  }
}
```

RestApis

Global Operations

Resource path: `/global-config/services/rest`

Resource version: `1.0`

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action RestApis --global --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action RestApis --global --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action RestApis --global --actionName nextdescendents
```

read

Usage:

```
am> read RestApis --global
```

update

Usage:

```
am> update RestApis --global --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "defaultVersion" : {
      "title" : "Default Resource Version",
      "description" : "The API resource version to use when the REST request does not specify an
 explicit version. Choose from:<br><br><ul><li><code>Latest</code>. If an explicit version is not
 specified, the latest resource version of an API is used.</li><li><code>Oldest</code>. If an explicit
 version is not specified, the oldest supported resource version of an API is used. Note that since
 APIs may be deprecated and fall out of support, the oldest <i>supported</i> version may not be the
 first version.</li><li><code>None</code>. If an explicit version is not specified, the request will
 not be handled and an error status is returned.</li></ul>",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "csrfFilterEnabled" : {
      "title" : "Enable CSRF Protection",
      "description" : "If enabled, all non-read/query requests will require the X-Requested-With
 header to be present.<br><br>Requiring a non-standard header ensures requests can only be made via
 methods (XHR) that have stricter same-origin policy protections in Web browsers, preventing Cross-
Site Request Forgery (CSRF) attacks. Without this filter, cross-origin requests are prevented by the
 use of the application/json Content-Type header, which is less robust.",
      "propertyOrder" : 500,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "defaultProtocolVersion" : {
      "title" : "Default Protocol Version",
      "description" : "The API protocol version to use when a REST request does not specify an
 explicit version. Choose from:<br><br><ul><li><code>Oldest</code>. If an explicit version is not
 specified, the oldest protocol version is used.</li><li><code>Latest</code>. If an explicit version
 is not specified, the latest protocol version is used.</li><li><code>None</code>. If an explicit
 version is not specified, the request will not be handled and an error status is returned.</li></
ul>",
      "propertyOrder" : 400,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
```

```
    },
    "descriptionsState" : {
      "title" : "API Descriptions",
      "description" : "Whether API Explorer and API Docs are enabled in OpenAM and how the
 documentation for them is generated. Dynamic generation includes descriptions from any custom
 services and authentication modules you may have added. Static generation only includes services
 and authentication modules that were present when OpenAM was built. Note that dynamic documentation
 generation may not work in some application containers.",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "warningHeader" : {
      "title" : "Warning Header",
      "description" : "Whether to include a warning header in the response to a request which fails to
 include the <code>Accept-API-Version</code> header.",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    }
  }
}
```


RetryLimitDecision

Realm Operations

Resource path: `/realm-config/authentication/authenticationtrees/nodes/RetryLimitDecisionNode`

Resource version: `1.0`

create

Usage:

```
am> create RetryLimitDecision --realm Realm --id id --body body
```

Parameters:

`--id`

The unique identifier for the resource.

`--body`

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "incrementUserAttributeOnFailure" : {
      "title" : "Save Retry Limit to User",
      "description" : "If true the number of failures will be persisted beyond the scope of the
 execution of this tree by saving them to an attribute on the user. If no user can be identified as
 part of the tree context then the execution of the tree will end with an error. If this is false then
 failures will be only be stored in the context of the current tree execution and will be lost if the
 tree execution is restarted.",
      "propertyOrder" : 200,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "retryLimit" : {
      "title" : "Retry Limit",
      "description" : "The number of times to allow a retry.",
      "propertyOrder" : 100,
      "type" : "integer",
      "exampleValue" : ""
    }
  },
  "required" : [ "incrementUserAttributeOnFailure", "retryLimit" ]
}
```

delete

Usage:

```
am> delete RetryLimitDecision --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action RetryLimitDecision --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action RetryLimitDecision --realm Realm --actionName getCreatableTypes
```

listOutcomes

List the available outcomes for the node type.

Usage:

```
am> action RetryLimitDecision --realm Realm --body body --actionName listOutcomes
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "title" : "Some configuration of the node. This does not need to be complete against the
 configuration schema."
}
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action RetryLimitDecision --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query RetryLimitDecision --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read RetryLimitDecision --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update RetryLimitDecision --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "incrementUserAttributeOnFailure" : {
      "title" : "Save Retry Limit to User",
      "description" : "If true the number of failures will be persisted beyond the scope of the
 execution of this tree by saving them to an attribute on the user. If no user can be identified as
 part of the tree context then the execution of the tree will end with an error. If this is false then
 failures will be only be stored in the context of the current tree execution and will be lost if the
 tree execution is restarted.",
      "propertyOrder" : 200,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "retryLimit" : {
      "title" : "Retry Limit",
      "description" : "The number of times to allow a retry.",
      "propertyOrder" : 100,
      "type" : "integer",
      "exampleValue" : ""
    }
  },
  "required" : [ "incrementUserAttributeOnFailure", "retryLimit" ]
}
```

SAML2Authentication

Realm Operations

Resource path: `/realm-config/authentication/authenticationtrees/nodes/product-Saml2Node`

Resource version: `1.0`

create

Usage:

```
am> create SAML2Authentication --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "binding" : {
      "title" : "Response Binding",
      "description" : "Use this parameter to indicate what binding the IdP should use when
 communicating with this SP.",
      "propertyOrder" : 800,
      "type" : "string",
      "exampleValue" : ""
    },
    "isPassive" : {
      "title" : "Passive Authentication",
      "description" : "Use this parameter to indicate whether the identity provider should
 authenticate passively (true) or not (false).",
      "propertyOrder" : 1000,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "authnContextDeclRef" : {
      "title" : "Authentication Context Declaration Reference",
      "description" : "(Optional) Use this parameter to specify authentication context declaration
 references.",
      "propertyOrder" : 600,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "idpEntityId" : {
      "title" : "IdP Entity ID",
      "description" : "The entity name of the SAML2 IdP Service to use for this module (must be
 configured).",
      "propertyOrder" : 100,
      "type" : "string",
      "exampleValue" : ""
    },
    "nameIdFormat" : {
      "title" : "NameID Format",
      "description" : "(Optional) Use this parameter to specify a SAML Name
 Identifier format identifier such as <pre>urn:oasis:names:tc:SAML:2.0:nameid-
format:persistent</pre> <pre>urn:oasis:names:tc:SAML:2.0:nameid-format:transient</pre>
 <pre>urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified</pre>",
      "propertyOrder" : 1100,
```

```
      "type" : "string",
      "exampleValue" : ""
    },
    "forceAuthn" : {
      "title" : "Force IdP Authentication",
      "description" : "Use this parameter to indicate whether the identity provider should force
 authentication (true) or can reuse existing security contexts (false).",
      "propertyOrder" : 900,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "metaAlias" : {
      "title" : "SP MetaAlias",
      "description" : "MetaAlias for Service Provider. The format of this parameter is <pre>/
realm_name/SP</pre>",
      "propertyOrder" : 200,
      "type" : "string",
      "exampleValue" : ""
    },
    "sloEnabled" : {
      "title" : "Single Logout Enabled",
      "description" : "Enable to attempt logout of the user's IdP session at the point of session
 logout.",
      "propertyOrder" : 1200,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "allowCreate" : {
      "title" : "Allow IdP to Create NameID",
      "description" : "Use this parameter to indicate whether the identity provider can create a new
 identifier for the principal if none exists (true) or not (false).",
      "propertyOrder" : 300,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "requestBinding" : {
      "title" : "Request Binding",
      "description" : "Use this parameter to indicate what binding the SP should use when
 communicating with the IdP.",
      "propertyOrder" : 700,
      "type" : "string",
      "exampleValue" : ""
    },
    "authnContextClassRef" : {
      "title" : "Authentication Context Class Reference",
      "description" : "(Optional) Use this parameter to specify authentication context class
 references.",
      "propertyOrder" : 500,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "sloRelayState" : {
      "title" : "Single Logout URL",
      "description" : "If Single Logout is enabled, this is the URL to which the user should be
 forwarded after successful IdP logout. This must be an absolute URL, or the redirect will not
 function.",
```

```
      "propertyOrder" : 1500,
      "type" : "string",
      "exampleValue" : ""
    },
    "authComparison" : {
      "title" : "Comparison Type",
      "description" : "(Optional) Use this parameter to specify a comparison method to evaluate the
 requested context classes or statements. OpenAM accepts the following values: <pre>better</pre>,
 <pre>exact</pre>, <pre>maximum</pre>, and <pre>minimum</pre>.",
      "propertyOrder" : 400,
      "type" : "string",
      "exampleValue" : ""
    }
  },
  "required" : [ "nameIdFormat", "allowCreate", "authnContextClassRef", "isPassive", "sloEnabled",
 "idpEntityId", "requestBinding", "authComparison", "metaAlias", "authnContextDeclRef", "forceAuthn",
 "binding" ]
}
```


delete

Usage:

```
am> delete SAML2Authentication --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action SAML2Authentication --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action SAML2Authentication --realm Realm --actionName getCreatableTypes
```

listOutcomes

List the available outcomes for the node type.

Usage:

```
am> action SAML2Authentication --realm Realm --body body --actionName listOutcomes
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "title" : "Some configuration of the node. This does not need to be complete against the
 configuration schema."
}
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action SAML2Authentication --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query SAML2Authentication --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read SAML2Authentication --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update SAML2Authentication --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "binding" : {
      "title" : "Response Binding",
      "description" : "Use this parameter to indicate what binding the IdP should use when
 communicating with this SP.",
      "propertyOrder" : 800,
      "type" : "string",
      "exampleValue" : ""
    },
    "isPassive" : {
      "title" : "Passive Authentication",
      "description" : "Use this parameter to indicate whether the identity provider should
 authenticate passively (true) or not (false).",
      "propertyOrder" : 1000,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "authnContextDeclRef" : {
      "title" : "Authentication Context Declaration Reference",
      "description" : "(Optional) Use this parameter to specify authentication context declaration
 references.",
      "propertyOrder" : 600,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "idpEntityId" : {
      "title" : "IdP Entity ID",
      "description" : "The entity name of the SAML2 IdP Service to use for this module (must be
 configured).",
      "propertyOrder" : 100,
      "type" : "string",
      "exampleValue" : ""
    },
    "nameIdFormat" : {
      "title" : "NameID Format",
      "description" : "(Optional) Use this parameter to specify a SAML Name
 Identifier format identifier such as <pre>urn:oasis:names:tc:SAML:2.0:nameid-
format:persistent</pre> <pre>urn:oasis:names:tc:SAML:2.0:nameid-format:transient</pre>
 <pre>urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified</pre>",
      "propertyOrder" : 1100,
```

```
      "type" : "string",
      "exampleValue" : ""
    },
    "forceAuthn" : {
      "title" : "Force IdP Authentication",
      "description" : "Use this parameter to indicate whether the identity provider should force
 authentication (true) or can reuse existing security contexts (false).",
      "propertyOrder" : 900,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "metaAlias" : {
      "title" : "SP MetaAlias",
      "description" : "MetaAlias for Service Provider. The format of this parameter is <pre>/
realm_name/SP</pre>",
      "propertyOrder" : 200,
      "type" : "string",
      "exampleValue" : ""
    },
    "sloEnabled" : {
      "title" : "Single Logout Enabled",
      "description" : "Enable to attempt logout of the user's IdP session at the point of session
 logout.",
      "propertyOrder" : 1200,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "allowCreate" : {
      "title" : "Allow IdP to Create NameID",
      "description" : "Use this parameter to indicate whether the identity provider can create a new
 identifier for the principal if none exists (true) or not (false).",
      "propertyOrder" : 300,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "requestBinding" : {
      "title" : "Request Binding",
      "description" : "Use this parameter to indicate what binding the SP should use when
 communicating with the IdP.",
      "propertyOrder" : 700,
      "type" : "string",
      "exampleValue" : ""
    },
    "authnContextClassRef" : {
      "title" : "Authentication Context Class Reference",
      "description" : "(Optional) Use this parameter to specify authentication context class
 references.",
      "propertyOrder" : 500,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "sloRelayState" : {
      "title" : "Single Logout URL",
      "description" : "If Single Logout is enabled, this is the URL to which the user should be
 forwarded after successful IdP logout. This must be an absolute URL, or the redirect will not
 function.",
```

```
      "propertyOrder" : 1500,
      "type" : "string",
      "exampleValue" : ""
    },
    "authComparison" : {
      "title" : "Comparison Type",
      "description" : "(Optional) Use this parameter to specify a comparison method to evaluate the
 requested context classes or statements. OpenAM accepts the following values: <pre>better</pre>,
 <pre>exact</pre>, <pre>maximum</pre>, and <pre>minimum</pre>.",
      "propertyOrder" : 400,
      "type" : "string",
      "exampleValue" : ""
    }
  },
  "required" : [ "nameIdFormat", "allowCreate", "authnContextClassRef", "isPassive", "sloEnabled",
 "idpEntityId", "requestBinding", "authComparison", "metaAlias", "authnContextDeclRef", "forceAuthn",
 "binding" ]
}
```

SOAPSecurityTokenServices

Realm Operations

The SOAP STS endpoint is responsible for storing the configuration of instances of REST Security Token Services (STS). Available operations are create, read, update, delete, query, schema and template.

Resource path: `/realm-config/services/sts/soap-sts`

Resource version: `1.0`

create

Usage:

```
am> create SOAPSecurityTokenServices --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "soapStsOidc" : {
```

```
      "type" : "object",
      "title" : "OpenID Connect Token ",
      "propertyOrder" : 4,
      "properties" : {
        "oidc-audience" : {
          "title" : "Issued Tokens Audience",
          "description" : "Contents will be set in the aud claim",
          "propertyOrder" : 5900,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "oidc-claim-map" : {
          "title" : "Claim Map",
          "description" : "Contains the mapping of OIDC token claim names (Map keys) to local
 OpenAM attributes (Map values) in configured data stores. Format: <code>claim_name=attribute_name</
code><br><br>The keys in the map will be claim entries in the issued OIDC token, and the value of
 these claims will be the principal attribute state resulting from LDAP datastore lookup of the map
 values. If no values are returned from the LDAP datastore lookup of the attribute corresponding to
 the map value, no claim will be set in the issued OIDC token.",
          "propertyOrder" : 6100,
          "required" : false,
          "patternProperties" : {
            ".*" : {
              "type" : "string"
            }
          },
          "type" : "object",
          "exampleValue" : ""
        },
        "oidc-issuer" : {
          "title" : "OpenID Connect Token Provider ID",
          "description" : "",
          "propertyOrder" : 4700,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "oidc-custom-authn-method-references-mapper-class" : {
          "title" : "Custom Authn Methods References Mapper Class",
          "description" : "If issued OIDC tokens are to contain amr claims, implement the
 <code>org.forgerock.openam.sts.rest.token.provider.oidc.OpenIdConnectTokenAuthMethodReferencesMapper</
code> interface, and specify the class name of the implementation here.",
          "propertyOrder" : 6400,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "oidc-custom-claim-mapper-class" : {
          "title" : "Custom Claim Mapper Class",
          "description" : "",
          "propertyOrder" : 6200,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
```

```
        "oidc-signature-key-alias" : {
          "title" : "KeyStore Signing Key Alias",
          "description" : "For RSA-signed tokens, corresponds to the private key of the OIDC OP. Will
 be used to sign assertions.",
          "propertyOrder" : 5400,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "oidc-custom-authn-context-mapper-class" : {
          "title" : "Custom Authn Context Mapper Class",
          "description" : "If issued OIDC tokens are to contain acr claims, implement the
 <code>org.forgerock.openam.sts.rest.token.provider.oidc.OpenIdConnectTokenAuthnContextMapper</code>
 interface, and specify the class name of the implementation here.",
          "propertyOrder" : 6300,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "oidc-public-key-reference-type" : {
          "title" : "Public Key Reference Type",
          "description" : "For tokens signed with RSA, how should corresponding public key be
 referenced in the issued jwt",
          "propertyOrder" : 5000,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "oidc-signature-algorithm" : {
          "title" : "Token Signature Algorithm",
          "description" : "Algorithm used to sign issued OIDC tokens",
          "propertyOrder" : 4900,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "oidc-keystore-location" : {
          "title" : "KeyStore Location",
          "description" : "For RSA-signed tokens, the filesystem or classpath location of the KeyStore
 containing signing key entry<br><br>For RSA-signed tokens, the KeyStore location, password, signing-
key alias, and signing key password must be specified. The client secret is not required for RSA-
signed tokens.",
          "propertyOrder" : 5100,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "oidc-token-lifetime-seconds" : {
          "title" : "Token Lifetime (Seconds)",
          "description" : "",
          "propertyOrder" : 4800,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "oidc-signature-key-password" : {
          "title" : "Signature Key Password",
          "description" : "",
          "propertyOrder" : 5500,
```

```
          "required" : true,
          "type" : "string",
          "format" : "password",
          "exampleValue" : ""
        },
        "oidc-client-secret" : {
          "title" : "Client Secret",
          "description" : "For HMAC-signed tokens, the client secret used as the HMAC key<br><br>For
 HMAC-signed tokens, the KeyStore location, password, signature key alias and password configurations
 are not required.",
          "propertyOrder" : 5700,
          "required" : true,
          "type" : "string",
          "format" : "password",
          "exampleValue" : ""
        },
        "oidc-authorized-party" : {
          "title" : "Authorized Party ",
          "description" : "Optional. Will be set in the azp claim",
          "propertyOrder" : 6000,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "oidc-keystore-password" : {
          "title" : "KeyStore Password",
          "description" : "",
          "propertyOrder" : 5200,
          "required" : true,
          "type" : "string",
          "format" : "password",
          "exampleValue" : ""
        }
      }
    },
    "soapStsSaml2" : {
      "type" : "object",
      "title" : "SAML2 Token",
      "propertyOrder" : 3,
      "properties" : {
        "saml2-key-transport-algorithm" : {
          "title" : "Key Transport Algorithm",
          "description" : "This setting controls the encryption algorithm used to encrypt the
 symmetric encryption key when SAML2 token encryption is enabled. Valid values include: <pre>http://
www.w3.org/2001/04/xmlenc#rsa-1_5</pre>, <pre>http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p</pre>,
 and <pre>http://www.w3.org/2009/xmlenc11#rsa-oaep</pre>",
          "propertyOrder" : 4060,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "saml2-custom-authentication-statements-provider-class-name" : {
          "title" : "Custom AuthenticationStatements Class Name",
          "description" : "If the AuthenticationStatements of
 the issued SAML2 assertion need to be customized, implement the
 <code>org.forgerock.openam.sts.tokengeneration.saml2.statements.AuthenticationStatementsProvider</
code> interface, and specify the class name of the implementation here.",
          "propertyOrder" : 3000,
          "required" : false,
```

```
          "type" : "string",
          "exampleValue" : ""
        },
        "saml2-sp-acs-url" : {
          "title" : "Service Provider Assertion Consumer Service Url",
          "description" : "When issuing bearer assertions, the recipient attribute of the
SubjectConfirmation element must be set to the Service Provider Assertion Consumer Service Url. See
section 4.1.4.2 of Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0 for details.
Value required when issuing Bearer assertions.",
          "propertyOrder" : 2500,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "issuer-name" : {
          "title" : "SAML2 issuer Id",
          "description" : "",
          "propertyOrder" : 2300,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "saml2-sp-entity-id" : {
          "title" : "Service Provider Entity Id",
          "description" : "Values will be used to populate the Audiences of the AudienceRestriction
element of the Conditions element. This value is required when issuing Bearer assertions. See section
4.1.4.2 of Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0 for details.",
          "propertyOrder" : 2400,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "saml2-sign-assertion" : {
          "title" : "Sign Assertion",
          "description" : "",
          "propertyOrder" : 3600,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "saml2-signature-key-password" : {
          "title" : "Signature Key Password",
          "description" : "",
          "propertyOrder" : 4600,
          "required" : false,
          "type" : "string",
          "format" : "password",
          "exampleValue" : ""
        },
        "saml2-custom-conditions-provider-class-name" : {
          "title" : "Custom Conditions Provider Class Name ",
          "description" : "If the Conditions of the issued SAML2 assertion need to be customized,
implement the org.forgerock.openam.sts.tokengeneration.saml2.statements.ConditionsProvider interface,
and specify the class name of the implementation here.",
          "propertyOrder" : 2800,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
```

```
       "saml2-keystore-filename" : {
         "title" : "KeystorePath",
         "description" : "Path to keystore<br><br>Provide either the full filesystem path to a
filesystem resident keystore, or a classpath-relative path to a keystore bundled in the OpenAM .war
file. This keystore contains the IdP public/private keys and SP public key for signed and/or
encrypted assertions. If assertions are neither signed nor encrypted, these values need not be
specified.",
         "propertyOrder" : 4100,
         "required" : false,
         "type" : "string",
         "exampleValue" : ""
       },
       "saml2-name-id-format" : {
         "title" : "NameIdFormat",
         "description" : "",
         "propertyOrder" : 2600,
         "required" : true,
         "type" : "string",
         "exampleValue" : ""
       },
       "saml2-signature-key-alias" : {
         "title" : "Signature Key Alias",
         "description" : "Corresponds to the private key of the IdP. Will be used to sign assertions.
Value can remain unspecified unless assertions are signed.",
         "propertyOrder" : 4500,
         "required" : true,
         "type" : "string",
         "exampleValue" : ""
       },
       "saml2-encrypt-assertion" : {
         "title" : "Encrypt Assertion",
         "description" : "Check this box if the entire assertion should be encrypted. If this box is
checked, the Encrypt NameID and Encrypt Attributes boxes cannot be checked.",
         "propertyOrder" : 3700,
         "required" : false,
         "type" : "boolean",
         "exampleValue" : ""
       },
       "saml2-encrypt-attributes" : {
         "title" : "Encrypt Attributes",
         "description" : "Check this box if the assertion Attributes should be encrypted. If this box
is checked, the Encrypt Assertion box cannot be checked.",
         "propertyOrder" : 3800,
         "required" : false,
         "type" : "boolean",
         "exampleValue" : ""
       },
       "saml2-custom-attribute-mapper-class-name" : {
         "title" : "Custom Attribute Mapper Class Name",
         "description" : "If the class implementing attribute mapping for attributes
contained in the issued SAML2 assertion needs to be customized, implement the
<code>org.forgerock.openam.sts.tokengeneration.saml2.statements.AttributeMapper</code> interface, and
specify the class name of the implementation here.",
         "propertyOrder" : 3300,
         "required" : false,
         "type" : "string",
         "exampleValue" : ""
       },
       "saml2-custom-subject-provider-class-name" : {
```

```
          "title" : "Custom Subject Provider Class Name ",
          "description" : "If the Subject of the issued SAML2 assertion needs to be customized,
 implement the org.forgerock.openam.sts.tokengeneration.saml2.statements.SubjectProvider interface,
 and specify the class name of the implementation here.",
          "propertyOrder" : 2900,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "saml2-encryption-algorithm" : {
          "title" : "Encryption Algorithm",
          "description" : "Algorithm used to encrypt generated assertions.",
          "propertyOrder" : 4000,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "saml2-custom-attribute-statements-provider-class-name" : {
          "title" : "Custom AttributeStatements Class Name",
          "description" : "If the AttributeStatements of the
 issued SAML2 assertion need to be customized, implement the
 <code>org.forgerock.openam.sts.tokengeneration.saml2.statements.AttributeStatementsProvider</code>
 interface, and specify the class name of the implementation here.",
          "propertyOrder" : 3100,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "saml2-custom-authz-decision-statements-provider-class-name" : {
          "title" : "Custom Authorization Decision Statements Class Name",
          "description" : "If the AuthorizationDecisionStatements
 of the issued SAML2 assertion need to be customized, implement the
 <code>org.forgerock.openam.sts.tokengeneration.saml2.statements.AuthzDecisionStatementsProvider</
code> interface, and specify the class name of the implementation here.",
          "propertyOrder" : 3200,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "saml2-custom-authn-context-mapper-class-name" : {
          "title" : "Custom Authentication Context Class Name",
          "description" : "If the AuthnContext mapping implemented by the
 <code>org.forgerock.openam.sts.soap.token.provider.saml2.DefaultSaml2XmlTokenAuthnContextMapper</
code> class needs to be customized, implement the
 <code>org.forgerock.openam.sts.soap.token.provider.saml2.Saml2XmlTokenAuthnContextMapper</code>
 interface, and specify the name of the implementation here.",
          "propertyOrder" : 3400,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "saml2-encrypt-nameid" : {
          "title" : "Encrypt NameID",
          "description" : "Check this box if the assertion NameID should be encrypted. If this box is
 checked, the Encrypt Assertion box cannot be checked.",
          "propertyOrder" : 3900,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
```

```
        },
        "saml2-keystore-password" : {
          "title" : "Keystore Password",
          "description" : "",
          "propertyOrder" : 4200,
          "required" : false,
          "type" : "string",
          "format" : "password",
          "exampleValue" : ""
        },
        "saml2-attribute-map" : {
          "title" : "Attribute Mappings",
          "description" : "Contains the mapping of assertion attribute names (Map
 keys) to local OpenAM attributes (Map values) in configured data stores.<br>Format:
 <code>assertion_attr_name=ldap_attr_name</code><br><br>The DefaultAttributeMapper looks at
 profile attributes in configured data stores, or in Session properties. The keys will define
 the name of the attributes included in the Assertion Attribute statements, and the data
 pulled from the subject's directory entry or session state corresponding to the map value
 will define the value corresponding to this attribute name. The keys can have the format
 <code>[NameFomatURI|]SAML ATTRIBUTE NAME.</code> If the attribute value is enclosed in quotes,
 that quoted value will be included in the attribute without mapping. Binary attributes should
 be followed by ';binary'.<br>Examples: <ul><li>EmailAddress=mail</li><li>Address=postaladdress</
li><li>urn:oasis:names:tc:SAML:2.0:attrname-format:uri|urn:mace:dir:attribute-def:cn=cn</
li><li>partnerID=\"staticPartnerIDValue\"</li><li>urn:oasis:names:tc:SAML:2.0:attrname-format:uri|
nameID=\"staticNameIDValue\"</li><li>photo=photo;binary</li><li>urn:oasis:names:tc:SAML:2.0:attrname-
format:uri|photo=photo;binary</li></ul>",
          "propertyOrder" : 3500,
          "required" : false,
          "patternProperties" : {
            ".*" : {
              "type" : "string"
            }
          },
          "type" : "object",
          "exampleValue" : ""
        },
        "saml2-token-lifetime-seconds" : {
          "title" : "Token Lifetime (Seconds)",
          "description" : "",
          "propertyOrder" : 2700,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "saml2-encryption-key-alias" : {
          "title" : "Encryption Key Alias",
          "description" : "This alias corresponds to the SP's x509 Certificate identified by the SP
 Entity ID for this rest-sts instance. Not necessary unless assertions are to be encrypted.",
          "propertyOrder" : 4400,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "soapStsGeneral" : {
      "type" : "object",
      "title" : "General",
      "propertyOrder" : 0,
```

```
     "properties" : {
       "security-policy-validated-token-config" : {
         "title" : "Security Policy Validated Token",
         "description" : "Determines the SupportingToken type in the WS-SecurityPolicy bindings in
the soap STS' wsdl, and whether the interim OpenAM session resulting from successful SupportingToken
validation, should be invalidated following token issue.",
         "propertyOrder" : 300,
         "required" : true,
         "items" : {
           "type" : "string"
         },
         "minItems" : 1,
         "type" : "array",
         "exampleValue" : ""
       },
       "issued-token-types" : {
         "title" : "Issued Tokens",
         "description" : "Determines which tokens this soap STS instance will issue",
         "propertyOrder" : 200,
         "required" : true,
         "items" : {
           "type" : "string"
         },
         "type" : "array",
         "exampleValue" : ""
       },
       "persist-issued-tokens-in-cts" : {
         "title" : "Persist Issued Tokens in Core Token Store",
         "description" : "Necessary to support token validation and cancellation<br><br>Validation of
STS-issued tokens will involve determining whether the token has been issued, has not expired, and
has not been cancelled. Token cancellation involves removing the record of this token from the CTS.
Thus CTS persistence of STS-issued tokens is required to support these features.",
         "propertyOrder" : 100,
         "required" : false,
         "type" : "boolean",
         "exampleValue" : ""
       }
     }
   },
   "soapStsSoap" : {
     "type" : "object",
     "title" : "Soap Keystore",
     "propertyOrder" : 2,
     "properties" : {
       "soap-signature-key-alias" : {
         "title" : "Signature Key Alias",
         "description" : "Alias of key used to sign messages from STS. Necessary for asymmetric
binding.",
         "propertyOrder" : 1700,
         "required" : true,
         "type" : "string",
         "exampleValue" : ""
       },
       "soap-signature-key-password" : {
         "title" : "Signature Key Password",
         "description" : "",
         "propertyOrder" : 1800,
         "required" : false,
         "type" : "string",
```

```
          "format" : "password",
          "exampleValue" : ""
        },
        "soap-keystore-password" : {
          "title" : "Keystore Password",
          "description" : "",
          "propertyOrder" : 1500,
          "required" : false,
          "type" : "string",
          "format" : "password",
          "exampleValue" : ""
        },
        "soap-keystore-filename" : {
          "title" : "Soap Keystore Location",
          "description" : "The location of the keystore which contains the key state necessary for the
 CXF and WSS4j runtime to enforce the SecurityPolicy bindings associated with this STS instance.",
          "propertyOrder" : 1400,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "soap-encryption-key-password" : {
          "title" : "Decryption Key Password",
          "description" : "",
          "propertyOrder" : 2100,
          "required" : false,
          "type" : "string",
          "format" : "password",
          "exampleValue" : ""
        },
        "soap-encryption-key-alias" : {
          "title" : "Decryption Key Alias",
          "description" : "Alias of key used by the STS to decrypt client messages in the asymmetric
 binding, and to decrypt the client-generated symmetric key in the symmetric binding. Corresponds to
 an STS PrivateKeyEntry.",
          "propertyOrder" : 2000,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "soapStsDeployment" : {
      "type" : "object",
      "title" : "Deployment",
      "propertyOrder" : 1,
      "properties" : {
        "deployment-custom-service-name" : {
          "title" : "Custom Service QName",
          "description" : "The name attribute of the wsdl:Service element referenced in the
 Custom wsdl File, in QName format.<br><br>Example: <code>{http://docs.oasis-open.org/ws-sx/ws-
trust/200512/}service_name</code>",
          "propertyOrder" : 900,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "delegation-relationship-supported" : {
          "title" : "Delegation Relationships Supported",
```

```
          "description" : "Check if the RST will include ActAs/OnBehalfOf token elements<br><br>If
 SAML2 assertions with SenderVouches SubjectConfirmation are to be issued, this box must be checked.",
          "propertyOrder" : 1100,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "deployment-am-url" : {
          "title" : "OpenAM URL",
          "description" : "Set to URL of the OpenAM instance or site deployment.<br><br>The OpenAM
 deployment will be consulted for published soap-sts instances, and to authenticate and issue
 tokens.",
          "propertyOrder" : 600,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "deployment-auth-target-mappings" : {
          "title" : "Authentication Target Mappings",
          "description" : "Configuration of consumption of OpenAM's rest-authN<br><br>Each deployed
 STS is configured with the authentication targets for each input token type for each supported
 token transformation. For example, if the transformation OPENIDCONNECT->SAML2 is supported, the
 STS instance must be configured with information specifying which elements of the OpenAM restful
 authentication context needs to be consumed to validate the OPENIDCONNECT token. The elements
 of the configuration tuple are separated by '|'. <br>The first element is the input token type
 in the token transform: i.e. X509, OPENIDCONNECT, USERNAME, or OPENAM. The second element is the
 authentication target - i.e. either 'module' or 'service', and the third element is the name of
 the authentication module or service. The fourth (optional) element provides the STS authentication
 context information about the to-be-consumed authentication context. <r>When transforming OpenID
 Connect Id tokens, the OpenID Connect authentication module must be consumed, and thus a deployed
 rest-sts instance must be configured with the name of the header/cookie element where the OpenID
 Connect Id token will be placed. For this example, the following string would define these
 configurations: <code>OPENIDCONNECT|module|oidc|oidc_id_token_auth_target_header_key=oidc_id_token</
code>. In this case, 'oidc' is the name of the OpenID Connect authentication module created to
 authenticate OpenID Connect tokens. <br>When transforming a X509 Certificate, the Certificate
 module must be consumed, and the published rest-sts instance must be configured with the name of
 the Certificate module (or the service containing the module), and the header name configured for
 the Certificate module corresponding to where the Certificate module can expect to find the to-be-
validated Certificate. The following string would define these configurations: <code>X509|module|
cert_module|x509_token_auth_target_header_key=client_cert</code>. In this case 'cert_module' is the
 name of the Certificate module, and client_cert is the header name where Certificate module has been
 configured to find the client's Certificate.",
          "propertyOrder" : 500,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "minItems" : 1,
          "type" : "array",
          "exampleValue" : ""
        },
        "deployment-wsdl-location" : {
          "title" : "Wsdl File Referencing Security Policy Binding Selection",
          "description" : "Choose the SupportingToken type and corresponding SecurityPolicy binding
 which will protect your sts instance. This choice will determine the SecurityPolicy bindings in
 the wsdl file defining the WS-Trust API<br><br>Note that the SupportingToken type selected must
 correspond to the Security Policy Validated Token selection. Note if a custom wsdl file is chose, the
 user is responsible for providing a properly formatted wsdl file. See documentation for details.",
          "propertyOrder" : 700,
```

```
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "delegation-validated-token-types" : {
          "title" : "Delegated Token Types",
          "description" : "If delegation relationships are supported, out-of-the-box validation
 support for the validation of username and OpenAM session tokens included as the ActAs/OnBehalfOf
 element is configured here. If delegation relationships are supported, out-of-the-box validation
 support for the validation of username and OpenAM session tokens included as the ActAs/OnBehalfOf
 element is configured here.<br><br>If a value is selected in this list, then no Custom Delegation
 Handlers must be specified. The true/false value indicates whether the interim OpenAM session,
 created as part of delegated token validation, should be invalidated following token creation.",
          "propertyOrder" : 1200,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "deployment-custom-service-port" : {
          "title" : "Custom Port QName",
          "description" : "The name attribute of the wsdl:Port element referenced in the
 Custom wsdl File, in QName format.<br><br>Example: <code>{http://docs.oasis-open.org/ws-sx/ws-
trust/200512/}service_port_name</code>",
          "propertyOrder" : 1000,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "delegation-custom-token-handlers" : {
          "title" : "Custom Delegation Handlers ",
          "description" : "If delegation relationships are supported, the
 class names soap-sts .war file classpath resident implementations of the
 <code>org.apache.cxf.sts.token.delegation.TokenDelegationHandler</code> interface can be specified
 here.<br><br>Custom TokenDelegationHandler implementations will be invoked to validate the
 potentially custom token element included in the ActAs/OnBehalfOf element in the RequestSecurityToken
 invocation. Note that a TokenDelegationHandler does not need to be supplied to validate username or
 OpenAM session tokens. The validation of these tokens are supported out-of-the-box by selecting them
 in the Delegated Token Types list.",
          "propertyOrder" : 1300,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "deployment-custom-wsdl-location" : {
          "title" : "Custom wsdl File",
          "description" : "The location (on soap-sts .war accessible filesystem or soap-sts .war
 classpath) of the custom wsdl file.<br><br>If the signing and/or encryption of the request and/or
 response messages specified in the SecurityPolicy bindings of standard soap-sts wdsl files must
 be customized, specify the name of the customized wsdl file here. See documentation for additional
 details.",
          "propertyOrder" : 800,
          "required" : false,
          "type" : "string",
```

```
          "exampleValue" : ""
        }
      }
    }
  }
}
```

delete

Usage:

```
am> delete SOAPSecurityTokenServices --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action SOAPSecurityTokenServices --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action SOAPSecurityTokenServices --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action SOAPSecurityTokenServices --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query SOAPSecurityTokenServices --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read SOAPSecurityTokenServices --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update SOAPSecurityTokenServices --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "soapStsOidc" : {
      "type" : "object",
      "title" : "OpenID Connect Token ",
      "propertyOrder" : 4,
      "properties" : {
        "oidc-audience" : {
          "title" : "Issued Tokens Audience",
          "description" : "Contents will be set in the aud claim",
          "propertyOrder" : 5900,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "oidc-claim-map" : {
```

```
          "title" : "Claim Map",
          "description" : "Contains the mapping of OIDC token claim names (Map keys) to local
 OpenAM attributes (Map values) in configured data stores. Format: <code>claim_name=attribute_name</
code><br><br>The keys in the map will be claim entries in the issued OIDC token, and the value of
 these claims will be the principal attribute state resulting from LDAP datastore lookup of the map
 values. If no values are returned from the LDAP datastore lookup of the attribute corresponding to
 the map value, no claim will be set in the issued OIDC token.",
          "propertyOrder" : 6100,
          "required" : false,
          "patternProperties" : {
            ".*" : {
              "type" : "string"
            }
          },
          "type" : "object",
          "exampleValue" : ""
        },
        "oidc-issuer" : {
          "title" : "OpenID Connect Token Provider ID",
          "description" : "",
          "propertyOrder" : 4700,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "oidc-custom-authn-method-references-mapper-class" : {
          "title" : "Custom Authn Methods References Mapper Class",
          "description" : "If issued OIDC tokens are to contain amr claims, implement the
 <code>org.forgerock.openam.sts.rest.token.provider.oidc.OpenIdConnectTokenAuthMethodReferencesMapper</
code> interface, and specify the class name of the implementation here.",
          "propertyOrder" : 6400,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "oidc-custom-claim-mapper-class" : {
          "title" : "Custom Claim Mapper Class",
          "description" : "",
          "propertyOrder" : 6200,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "oidc-signature-key-alias" : {
          "title" : "KeyStore Signing Key Alias",
          "description" : "For RSA-signed tokens, corresponds to the private key of the OIDC OP. Will
 be used to sign assertions.",
          "propertyOrder" : 5400,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "oidc-custom-authn-context-mapper-class" : {
          "title" : "Custom Authn Context Mapper Class",
          "description" : "If issued OIDC tokens are to contain acr claims, implement the
 <code>org.forgerock.openam.sts.rest.token.provider.oidc.OpenIdConnectTokenAuthnContextMapper</code>
 interface, and specify the class name of the implementation here.",
          "propertyOrder" : 6300,
          "required" : false,
```

```
          "type" : "string",
          "exampleValue" : ""
        },
        "oidc-public-key-reference-type" : {
          "title" : "Public Key Reference Type",
          "description" : "For tokens signed with RSA, how should corresponding public key be
 referenced in the issued jwt",
          "propertyOrder" : 5000,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "oidc-signature-algorithm" : {
          "title" : "Token Signature Algorithm",
          "description" : "Algorithm used to sign issued OIDC tokens",
          "propertyOrder" : 4900,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "oidc-keystore-location" : {
          "title" : "KeyStore Location",
          "description" : "For RSA-signed tokens, the filesystem or classpath location of the KeyStore
 containing signing key entry<br><br>For RSA-signed tokens, the KeyStore location, password, signing-
key alias, and signing key password must be specified. The client secret is not required for RSA-
signed tokens.",
          "propertyOrder" : 5100,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "oidc-token-lifetime-seconds" : {
          "title" : "Token Lifetime (Seconds)",
          "description" : "",
          "propertyOrder" : 4800,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "oidc-signature-key-password" : {
          "title" : "Signature Key Password",
          "description" : "",
          "propertyOrder" : 5500,
          "required" : true,
          "type" : "string",
          "format" : "password",
          "exampleValue" : ""
        },
        "oidc-client-secret" : {
          "title" : "Client Secret",
          "description" : "For HMAC-signed tokens, the client secret used as the HMAC key<br><br>For
 HMAC-signed tokens, the KeyStore location, password, signature key alias and password configurations
 are not required.",
          "propertyOrder" : 5700,
          "required" : true,
          "type" : "string",
          "format" : "password",
          "exampleValue" : ""
        },
```

```
        "oidc-authorized-party" : {
          "title" : "Authorized Party ",
          "description" : "Optional. Will be set in the azp claim",
          "propertyOrder" : 6000,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "oidc-keystore-password" : {
          "title" : "KeyStore Password",
          "description" : "",
          "propertyOrder" : 5200,
          "required" : true,
          "type" : "string",
          "format" : "password",
          "exampleValue" : ""
        }
      }
    },
    "soapStsSaml2" : {
      "type" : "object",
      "title" : "SAML2 Token",
      "propertyOrder" : 3,
      "properties" : {
        "saml2-key-transport-algorithm" : {
          "title" : "Key Transport Algorithm",
          "description" : "This setting controls the encryption algorithm used to encrypt the
 symmetric encryption key when SAML2 token encryption is enabled. Valid values include: <pre>http://
www.w3.org/2001/04/xmlenc#rsa-1_5</pre>, <pre>http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p</pre>,
 and <pre>http://www.w3.org/2009/xmlenc11#rsa-oaep</pre>",
          "propertyOrder" : 4060,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "saml2-custom-authentication-statements-provider-class-name" : {
          "title" : "Custom AuthenticationStatements Class Name",
          "description" : "If the AuthenticationStatements of
 the issued SAML2 assertion need to be customized, implement the
 <code>org.forgerock.openam.sts.tokengeneration.saml2.statements.AuthenticationStatementsProvider</
code> interface, and specify the class name of the implementation here.",
          "propertyOrder" : 3000,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "saml2-sp-acs-url" : {
          "title" : "Service Provider Assertion Consumer Service Url",
          "description" : "When issuing bearer assertions, the recipient attribute of the
 SubjectConfirmation element must be set to the Service Provider Assertion Consumer Service Url. See
 section 4.1.4.2 of Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0 for details.
 Value required when issuing Bearer assertions.",
          "propertyOrder" : 2500,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "issuer-name" : {
          "title" : "SAML2 issuer Id",
```

```
          "description" : "",
          "propertyOrder" : 2300,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "saml2-sp-entity-id" : {
          "title" : "Service Provider Entity Id",
          "description" : "Values will be used to populate the Audiences of the AudienceRestriction
element of the Conditions element. This value is required when issuing Bearer assertions. See section
4.1.4.2 of Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0 for details.",
          "propertyOrder" : 2400,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "saml2-sign-assertion" : {
          "title" : "Sign Assertion",
          "description" : "",
          "propertyOrder" : 3600,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "saml2-signature-key-password" : {
          "title" : "Signature Key Password",
          "description" : "",
          "propertyOrder" : 4600,
          "required" : false,
          "type" : "string",
          "format" : "password",
          "exampleValue" : ""
        },
        "saml2-custom-conditions-provider-class-name" : {
          "title" : "Custom Conditions Provider Class Name ",
          "description" : "If the Conditions of the issued SAML2 assertion need to be customized,
implement the org.forgerock.openam.sts.tokengeneration.saml2.statements.ConditionsProvider interface,
and specify the class name of the implementation here.",
          "propertyOrder" : 2800,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "saml2-keystore-filename" : {
          "title" : "KeystorePath",
          "description" : "Path to keystore<br><br>Provide either the full filesystem path to a
filesystem resident keystore, or a classpath-relative path to a keystore bundled in the OpenAM .war
file. This keystore contains the IdP public/private keys and SP public key for signed and/or
encrypted assertions. If assertions are neither signed nor encrypted, these values need not be
specified.",
          "propertyOrder" : 4100,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "saml2-name-id-format" : {
          "title" : "NameIdFormat",
          "description" : "",
          "propertyOrder" : 2600,
```

```
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "saml2-signature-key-alias" : {
          "title" : "Signature Key Alias",
          "description" : "Corresponds to the private key of the IdP. Will be used to sign assertions.
Value can remain unspecified unless assertions are signed.",
          "propertyOrder" : 4500,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "saml2-encrypt-assertion" : {
          "title" : "Encrypt Assertion",
          "description" : "Check this box if the entire assertion should be encrypted. If this box is
checked, the Encrypt NameID and Encrypt Attributes boxes cannot be checked.",
          "propertyOrder" : 3700,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "saml2-encrypt-attributes" : {
          "title" : "Encrypt Attributes",
          "description" : "Check this box if the assertion Attributes should be encrypted. If this box
is checked, the Encrypt Assertion box cannot be checked.",
          "propertyOrder" : 3800,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "saml2-custom-attribute-mapper-class-name" : {
          "title" : "Custom Attribute Mapper Class Name",
          "description" : "If the class implementing attribute mapping for attributes
contained in the issued SAML2 assertion needs to be customized, implement the
<code>org.forgerock.openam.sts.tokengeneration.saml2.statements.AttributeMapper</code> interface, and
specify the class name of the implementation here.",
          "propertyOrder" : 3300,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "saml2-custom-subject-provider-class-name" : {
          "title" : "Custom Subject Provider Class Name ",
          "description" : "If the Subject of the issued SAML2 assertion needs to be customized,
implement the org.forgerock.openam.sts.tokengeneration.saml2.statements.SubjectProvider interface,
and specify the class name of the implementation here.",
          "propertyOrder" : 2900,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "saml2-encryption-algorithm" : {
          "title" : "Encryption Algorithm",
          "description" : "Algorithm used to encrypt generated assertions.",
          "propertyOrder" : 4000,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
```

```
        },
        "saml2-custom-attribute-statements-provider-class-name" : {
          "title" : "Custom AttributeStatements Class Name",
          "description" : "If the AttributeStatements of the
 issued SAML2 assertion need to be customized, implement the
 <code>org.forgerock.openam.sts.tokengeneration.saml2.statements.AttributeStatementsProvider</code>
 interface, and specify the class name of the implementation here.",
          "propertyOrder" : 3100,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "saml2-custom-authz-decision-statements-provider-class-name" : {
          "title" : "Custom Authorization Decision Statements Class Name",
          "description" : "If the AuthorizationDecisionStatements
 of the issued SAML2 assertion need to be customized, implement the
 <code>org.forgerock.openam.sts.tokengeneration.saml2.statements.AuthzDecisionStatementsProvider</
code> interface, and specify the class name of the implementation here.",
          "propertyOrder" : 3200,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "saml2-custom-authn-context-mapper-class-name" : {
          "title" : "Custom Authentication Context Class Name",
          "description" : "If the AuthnContext mapping implemented by the
 <code>org.forgerock.openam.sts.soap.token.provider.saml2.DefaultSaml2XmlTokenAuthnContextMapper</
code> class needs to be customized, implement the
 <code>org.forgerock.openam.sts.soap.token.provider.saml2.Saml2XmlTokenAuthnContextMapper</code>
 interface, and specify the name of the implementation here.",
          "propertyOrder" : 3400,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "saml2-encrypt-nameid" : {
          "title" : "Encrypt NameID",
          "description" : "Check this box if the assertion NameID should be encrypted. If this box is
 checked, the Encrypt Assertion box cannot be checked.",
          "propertyOrder" : 3900,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "saml2-keystore-password" : {
          "title" : "Keystore Password",
          "description" : "",
          "propertyOrder" : 4200,
          "required" : false,
          "type" : "string",
          "format" : "password",
          "exampleValue" : ""
        },
        "saml2-attribute-map" : {
          "title" : "Attribute Mappings",
          "description" : "Contains the mapping of assertion attribute names (Map
 keys) to local OpenAM attributes (Map values) in configured data stores.<br>Format:
 <code>assertion_attr_name=ldap_attr_name</code><br><br>The DefaultAttributeMapper looks at
 profile attributes in configured data stores, or in Session properties. The keys will define
```

```
 the name of the attributes included in the Assertion Attribute statements, and the data
 pulled from the subject's directory entry or session state corresponding to the map value
 will define the value corresponding to this attribute name. The keys can have the format
 <code>[NameFomatURI|]SAML ATTRIBUTE NAME.</code> If the attribute value is enclosed in quotes,
 that quoted value will be included in the attribute without mapping. Binary attributes should
 be followed by ';binary'.<br>Examples: <ul><li>EmailAddress=mail</li><li>Address=postaladdress</
li><li>urn:oasis:names:tc:SAML:2.0:attrname-format:uri|urn:mace:dir:attribute-def:cn=cn</
li><li>partnerID=\"staticPartnerIDValue\"</li><li>urn:oasis:names:tc:SAML:2.0:attrname-format:uri|
nameID=\"staticNameIDValue\"</li><li>photo=photo;binary</li><li>urn:oasis:names:tc:SAML:2.0:attrname-
format:uri|photo=photo;binary</li></ul>",
          "propertyOrder" : 3500,
          "required" : false,
          "patternProperties" : {
            ".*" : {
              "type" : "string"
            }
          },
          "type" : "object",
          "exampleValue" : ""
        },
        "saml2-token-lifetime-seconds" : {
          "title" : "Token Lifetime (Seconds)",
          "description" : "",
          "propertyOrder" : 2700,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "saml2-encryption-key-alias" : {
          "title" : "Encryption Key Alias",
          "description" : "This alias corresponds to the SP's x509 Certificate identified by the SP
 Entity ID for this rest-sts instance. Not necessary unless assertions are to be encrypted.",
          "propertyOrder" : 4400,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "soapStsGeneral" : {
      "type" : "object",
      "title" : "General",
      "propertyOrder" : 0,
      "properties" : {
        "security-policy-validated-token-config" : {
          "title" : "Security Policy Validated Token",
          "description" : "Determines the SupportingToken type in the WS-SecurityPolicy bindings in
 the soap STS' wsdl, and whether the interim OpenAM session resulting from successful SupportingToken
 validation, should be invalidated following token issue.",
          "propertyOrder" : 300,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "minItems" : 1,
          "type" : "array",
          "exampleValue" : ""
        },
        "issued-token-types" : {
```

```
          "title" : "Issued Tokens",
          "description" : "Determines which tokens this soap STS instance will issue",
          "propertyOrder" : 200,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "persist-issued-tokens-in-cts" : {
          "title" : "Persist Issued Tokens in Core Token Store",
          "description" : "Necessary to support token validation and cancellation<br><br>Validation of
STS-issued tokens will involve determining whether the token has been issued, has not expired, and
has not been cancelled. Token cancellation involves removing the record of this token from the CTS.
Thus CTS persistence of STS-issued tokens is required to support these features.",
          "propertyOrder" : 100,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        }
      }
    },
    "soapStsSoap" : {
      "type" : "object",
      "title" : "Soap Keystore",
      "propertyOrder" : 2,
      "properties" : {
        "soap-signature-key-alias" : {
          "title" : "Signature Key Alias",
          "description" : "Alias of key used to sign messages from STS. Necessary for asymmetric
binding.",
          "propertyOrder" : 1700,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "soap-signature-key-password" : {
          "title" : "Signature Key Password",
          "description" : "",
          "propertyOrder" : 1800,
          "required" : false,
          "type" : "string",
          "format" : "password",
          "exampleValue" : ""
        },
        "soap-keystore-password" : {
          "title" : "Keystore Password",
          "description" : "",
          "propertyOrder" : 1500,
          "required" : false,
          "type" : "string",
          "format" : "password",
          "exampleValue" : ""
        },
        "soap-keystore-filename" : {
          "title" : "Soap Keystore Location",
          "description" : "The location of the keystore which contains the key state necessary for the
CXF and WSS4j runtime to enforce the SecurityPolicy bindings associated with this STS instance.",
```

```
          "propertyOrder" : 1400,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "soap-encryption-key-password" : {
          "title" : "Decryption Key Password",
          "description" : "",
          "propertyOrder" : 2100,
          "required" : false,
          "type" : "string",
          "format" : "password",
          "exampleValue" : ""
        },
        "soap-encryption-key-alias" : {
          "title" : "Decryption Key Alias",
          "description" : "Alias of key used by the STS to decrypt client messages in the asymmetric
 binding, and to decrypt the client-generated symmetric key in the symmetric binding. Corresponds to
 an STS PrivateKeyEntry.",
          "propertyOrder" : 2000,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "soapStsDeployment" : {
      "type" : "object",
      "title" : "Deployment",
      "propertyOrder" : 1,
      "properties" : {
        "deployment-custom-service-name" : {
          "title" : "Custom Service QName",
          "description" : "The name attribute of the wsdl:Service element referenced in the
 Custom wsdl File, in QName format.<br><br>Example: <code>{http://docs.oasis-open.org/ws-sx/ws-
trust/200512/}service_name</code>",
          "propertyOrder" : 900,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "delegation-relationship-supported" : {
          "title" : "Delegation Relationships Supported",
          "description" : "Check if the RST will include ActAs/OnBehalfOf token elements<br><br>If
 SAML2 assertions with SenderVouches SubjectConfirmation are to be issued, this box must be checked.",
          "propertyOrder" : 1100,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "deployment-am-url" : {
          "title" : "OpenAM URL",
          "description" : "Set to URL of the OpenAM instance or site deployment.<br><br>The OpenAM
 deployment will be consulted for published soap-sts instances, and to authenticate and issue
 tokens.",
          "propertyOrder" : 600,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
```

```
        },
        "deployment-auth-target-mappings" : {
          "title" : "Authentication Target Mappings",
          "description" : "Configuration of consumption of OpenAM's rest-authN<br><br>Each deployed
 STS is configured with the authentication targets for each input token type for each supported
 token transformation. For example, if the transformation OPENIDCONNECT->SAML2 is supported, the
 STS instance must be configured with information specifying which elements of the OpenAM restful
 authentication context needs to be consumed to validate the OPENIDCONNECT token. The elements
 of the configuration tuple are separated by '|'. <br>The first element is the input token type
 in the token transform: i.e. X509, OPENIDCONNECT, USERNAME, or OPENAM. The second element is the
 authentication target - i.e. either 'module' or 'service', and the third element is the name of
 the authentication module or service. The fourth (optional) element provides the STS authentication
 context information about the to-be-consumed authentication context. <r>When transforming OpenID
 Connect Id tokens, the OpenID Connect authentication module must be consumed, and thus a deployed
 rest-sts instance must be configured with the name of the header/cookie element where the OpenID
 Connect Id token will be placed. For this example, the following string would define these
 configurations: <code>OPENIDCONNECT|module|oidc|oidc_id_token_auth_target_header_key=oidc_id_token</
code>. In this case, 'oidc' is the name of the OpenID Connect authentication module created to
 authenticate OpenID Connect tokens. <br>When transforming a X509 Certificate, the Certificate
 module must be consumed, and the published rest-sts instance must be configured with the name of
 the Certificate module (or the service containing the module), and the header name configured for
 the Certificate module corresponding to where the Certificate module can expect to find the to-be-
validated Certificate. The following string would define these configurations: <code>X509|module|
cert_module|x509_token_auth_target_header_key=client_cert</code>. In this case 'cert_module' is the
 name of the Certificate module, and client_cert is the header name where Certificate module has been
 configured to find the client's Certificate.",
          "propertyOrder" : 500,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "minItems" : 1,
          "type" : "array",
          "exampleValue" : ""
        },
        "deployment-wsdl-location" : {
          "title" : "Wsdl File Referencing Security Policy Binding Selection",
          "description" : "Choose the SupportingToken type and corresponding SecurityPolicy binding
 which will protect your sts instance. This choice will determine the SecurityPolicy bindings in
 the wsdl file defining the WS-Trust API<br><br>Note that the SupportingToken type selected must
 correspond to the Security Policy Validated Token selection. Note if a custom wsdl file is chose, the
 user is responsible for providing a properly formatted wsdl file. See documentation for details.",
          "propertyOrder" : 700,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "delegation-validated-token-types" : {
          "title" : "Delegated Token Types",
          "description" : "If delegation relationships are supported, out-of-the-box validation
 support for the validation of username and OpenAM session tokens included as the ActAs/OnBehalfOf
 element is configured here. If delegation relationships are supported, out-of-the-box validation
 support for the validation of username and OpenAM session tokens included as the ActAs/OnBehalfOf
 element is configured here.<br><br>If a value is selected in this list, then no Custom Delegation
 Handlers must be specified. The true/false value indicates whether the interim OpenAM session,
 created as part of delegated token validation, should be invalidated following token creation.",
          "propertyOrder" : 1200,
          "required" : true,
          "items" : {
```

```
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "deployment-custom-service-port" : {
          "title" : "Custom Port QName",
          "description" : "The name attribute of the wsdl:Port element referenced in the
 Custom wsdl File, in QName format.<br><br>Example: <code>{http://docs.oasis-open.org/ws-sx/ws-
trust/200512/}service_port_name</code>",
          "propertyOrder" : 1000,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "delegation-custom-token-handlers" : {
          "title" : "Custom Delegation Handlers ",
          "description" : "If delegation relationships are supported, the
 class names soap-sts .war file classpath resident implementations of the
 <code>org.apache.cxf.sts.token.delegation.TokenDelegationHandler</code> interface can be specified
 here.<br><br>Custom TokenDelegationHandler implementations will be invoked to validate the
 potentially custom token element included in the ActAs/OnBehalfOf element in the RequestSecurityToken
 invocation. Note that a TokenDelegationHandler does not need to be supplied to validate username or
 OpenAM session tokens. The validation of these tokens are supported out-of-the-box by selecting them
 in the Delegated Token Types list.",
          "propertyOrder" : 1300,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "deployment-custom-wsdl-location" : {
          "title" : "Custom wsdl File",
          "description" : "The location (on soap-sts .war accessible filesystem or soap-sts .war
 classpath) of the custom wsdl file.<br><br>If the signing and/or encryption of the request and/or
 response messages specified in the SecurityPolicy bindings of standard soap-sts wdsl files must
 be customized, specify the name of the customized wsdl file here. See documentation for additional
 details.",
          "propertyOrder" : 800,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    }
  }
}
```

SaeModule

Realm Operations

Resource path: `/realm-config/authentication/modules/sae`

Resource version: `1.0`

create

Usage:

```
am> create SaeModule --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "authenticationLevel" : {
      "title" : "Authentication Level",
      "description" : "The authentication level associated with this module.<br><br>Each
 authentication module has an authentication level that can be used to indicate the level of security
 associated with the module; 0 is the lowest (and the default).",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    }
  }
}
```

delete

Usage:

```
am> delete SaeModule --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action SaeModule --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action SaeModule --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action SaeModule --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query SaeModule --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read SaeModule --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update SaeModule --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "authenticationLevel" : {
      "title" : "Authentication Level",
      "description" : "The authentication level associated with this module.<br><br>Each
 authentication module has an authentication level that can be used to indicate the level of security
 associated with the module; 0 is the lowest (and the default).",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    }
  }
}
```

Global Operations

Resource path: `/global-config/authentication/modules/sae`

Resource version: `1.0`

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action SaeModule --global --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action SaeModule --global --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action SaeModule --global --actionName nextdescendents
```

read

Usage:

```
am> read SaeModule --global
```

update

Usage:

```
am> update SaeModule --global --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "defaults" : {
      "properties" : {
        "authenticationLevel" : {
          "title" : "Authentication Level",
          "description" : "The authentication level associated with this module.<br><br>Each
 authentication module has an authentication level that can be used to indicate the level of security
 associated with the module; 0 is the lowest (and the default).",
          "propertyOrder" : 100,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        }
      },
      "type" : "object",
      "title" : "Realm Defaults"
    }
  }
}
```

Saml2Entities

Realm Operations

This endpoint allows querying SAML2 entities configured in the system regardless of whether they are hosted or remote

Resource path: `/realm-config/saml2`

Resource version: `1.0`

query

Usage:

```
am> query Saml2Entities --realm Realm --filter filter
```

Parameters:

`--filter`

A CREST formatted query filter, where "true" will query all. Fields that can be queried: [*]

Saml2Entity

Realm Operations

Resource path: `/realm-config/federation/entityproviders/saml2`

Resource version: `1.0`

create

Usage:

```
am> create Saml2Entity --realm Realm --id id --body body
```

Parameters:

`--id`

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "metadata" : {
      "title" : "Metadata",
      "description" : "",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "entityConfig" : {
      "title" : "Entity Configuration",
      "description" : "",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
```

delete

Usage:

```
am> delete Saml2Entity --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query Saml2Entity --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read Saml2Entity --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update Saml2Entity --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "metadata" : {
      "title" : "Metadata",
      "description" : "",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "entityConfig" : {
      "title" : "Entity Configuration",
      "description" : "",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
```

Saml2Module

Realm Operations

Resource path: `/realm-config/authentication/modules/authSaml`

Resource version: `1.0`

create

Usage:

```
am> create Saml2Module --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "authnContextDeclRef" : {
      "title" : "Authentication Context Declaration Reference",
      "description" : "(Optional) Use this parameter to specify authentication context declaration
 references. Separate multiple values with pipe characters (|).",
      "propertyOrder" : 800,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "nameIdFormat" : {
      "title" : "NameID Format",
      "description" : "(Optional) Use this parameter to specify a SAML Name
 Identifier format identifier such as <pre>urn:oasis:names:tc:SAML:2.0:nameid-
format:persistent</pre> <pre>urn:oasis:names:tc:SAML:2.0:nameid-format:transient</pre>
 <pre>urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified</pre>",
      "propertyOrder" : 1300,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "reqBinding" : {
      "title" : "Request Binding",
      "description" : "Use this parameter to indicate what binding the SP should use when
 communicating with the IdP.",
      "propertyOrder" : 900,
      "required" : true,
```

```
      "type" : "string",
      "exampleValue" : ""
    },
    "sloEnabled" : {
      "title" : "Single Logout Enabled",
      "description" : "Enable to attempt logout of the user's
 IdP session at the point of session logout. Required the
 <pre>org.forgerock.openam.authentication.modules.saml2.SAML2PostAuthenticationPlugin</pre> to be
 active on the chain that includes this SAML2 module.",
      "propertyOrder" : 1400,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "forceAuthn" : {
      "title" : "Force IdP Authentication",
      "description" : "Use this parameter to indicate whether the identity provider should force
 authentication (true) or can reuse existing security contexts (false).",
      "propertyOrder" : 1100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "sloRelay" : {
      "title" : "Single Logout URL",
      "description" : "If Single Logout is enabled, this is the URL to which the user should be
 forwarded after successful IdP logout. This must be a fully-qualified URL (start with http...), or
 the redirect will not function.",
      "propertyOrder" : 1500,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "metaAlias" : {
      "title" : "SP MetaAlias",
      "description" : "MetaAlias for Service Provider. The format of this parameter is <pre>/
realm_name/SP</pre>",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "authComparison" : {
      "title" : "Comparison Type",
      "description" : "(Optional) Use this parameter to specify a comparison method to evaluate the
 requested context classes or statements. OpenAM accepts the following values: <pre>better</pre>,
 <pre>exact</pre>, <pre>maximum</pre>, and <pre>minimum</pre>.",
      "propertyOrder" : 600,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "entityName" : {
      "title" : "IdP Entity ID",
      "description" : "The entity name of the SAML2 IdP Service to use for this module (must be
 configured).",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
```

```
     "exampleValue" : ""
   },
   "allowCreate" : {
     "title" : "Allow IdP to Create NameID",
     "description" : "Use this parameter to indicate whether the identity provider can create a new
identifier for the principal if none exists (true) or not (false).",
     "propertyOrder" : 400,
     "required" : true,
     "type" : "string",
     "exampleValue" : ""
   },
   "authnContextClassRef" : {
     "title" : "Authentication Context Class Reference",
     "description" : "(Optional) Use this parameter to specify authentication context class
references. Separate multiple values with pipe characters (|).",
     "propertyOrder" : 700,
     "required" : true,
     "type" : "string",
     "exampleValue" : ""
   },
   "loginChain" : {
     "title" : "Linking Authentication Chain",
     "description" : "The authentication chain that will be executed when a user is required to be
authenticated locally to match their user account with that of a remotely authenticated assertion.",
     "propertyOrder" : 500,
     "required" : true,
     "type" : "string",
     "exampleValue" : ""
   },
   "authenticationLevel" : {
     "title" : "Authentication Level",
     "description" : "The authentication level associated with this module.<br><br>Each
authentication module has an authentication level that can be used to indicate the level of security
associated with the module; 0 is the lowest (and the default).",
     "propertyOrder" : 100,
     "required" : true,
     "type" : "integer",
     "exampleValue" : ""
   },
   "isPassive" : {
     "title" : "Passive Authentication",
     "description" : "Use this parameter to indicate whether the identity provider should
authenticate passively (true) or not (false).",
     "propertyOrder" : 1200,
     "required" : true,
     "type" : "string",
     "exampleValue" : ""
   },
   "binding" : {
     "title" : "Response Binding",
     "description" : "Use this parameter to indicate what binding the IdP should use when
communicating with this SP.",
     "propertyOrder" : 1000,
     "required" : true,
     "type" : "string",
     "exampleValue" : ""
   }
 }
```

```
}
```

delete

Usage:

```
am> delete Saml2Module --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action Saml2Module --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action Saml2Module --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action Saml2Module --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query Saml2Module --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read Saml2Module --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update Saml2Module --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "authnContextDeclRef" : {
      "title" : "Authentication Context Declaration Reference",
      "description" : "(Optional) Use this parameter to specify authentication context declaration
 references. Separate multiple values with pipe characters (|).",
      "propertyOrder" : 800,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "nameIdFormat" : {
      "title" : "NameID Format",
      "description" : "(Optional) Use this parameter to specify a SAML Name
 Identifier format identifier such as <pre>urn:oasis:names:tc:SAML:2.0:nameid-
format:persistent</pre> <pre>urn:oasis:names:tc:SAML:2.0:nameid-format:transient</pre>
 <pre>urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified</pre>",
      "propertyOrder" : 1300,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
```

```
    },
    "reqBinding" : {
      "title" : "Request Binding",
      "description" : "Use this parameter to indicate what binding the SP should use when
 communicating with the IdP.",
      "propertyOrder" : 900,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "sloEnabled" : {
      "title" : "Single Logout Enabled",
      "description" : "Enable to attempt logout of the user's
 IdP session at the point of session logout. Required the
 <pre>org.forgerock.openam.authentication.modules.saml2.SAML2PostAuthenticationPlugin</pre> to be
 active on the chain that includes this SAML2 module.",
      "propertyOrder" : 1400,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "forceAuthn" : {
      "title" : "Force IdP Authentication",
      "description" : "Use this parameter to indicate whether the identity provider should force
 authentication (true) or can reuse existing security contexts (false).",
      "propertyOrder" : 1100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "sloRelay" : {
      "title" : "Single Logout URL",
      "description" : "If Single Logout is enabled, this is the URL to which the user should be
 forwarded after successful IdP logout. This must be a fully-qualified URL (start with http...), or
 the redirect will not function.",
      "propertyOrder" : 1500,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "metaAlias" : {
      "title" : "SP MetaAlias",
      "description" : "MetaAlias for Service Provider. The format of this parameter is <pre>/
realm_name/SP</pre>",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "authComparison" : {
      "title" : "Comparison Type",
      "description" : "(Optional) Use this parameter to specify a comparison method to evaluate the
 requested context classes or statements. OpenAM accepts the following values: <pre>better</pre>,
 <pre>exact</pre>, <pre>maximum</pre>, and <pre>minimum</pre>.",
      "propertyOrder" : 600,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
```

```
   "entityName" : {
     "title" : "IdP Entity ID",
     "description" : "The entity name of the SAML2 IdP Service to use for this module (must be
configured).",
     "propertyOrder" : 200,
     "required" : true,
     "type" : "string",
     "exampleValue" : ""
   },
   "allowCreate" : {
     "title" : "Allow IdP to Create NameID",
     "description" : "Use this parameter to indicate whether the identity provider can create a new
identifier for the principal if none exists (true) or not (false).",
     "propertyOrder" : 400,
     "required" : true,
     "type" : "string",
     "exampleValue" : ""
   },
   "authnContextClassRef" : {
     "title" : "Authentication Context Class Reference",
     "description" : "(Optional) Use this parameter to specify authentication context class
references. Separate multiple values with pipe characters (|).",
     "propertyOrder" : 700,
     "required" : true,
     "type" : "string",
     "exampleValue" : ""
   },
   "loginChain" : {
     "title" : "Linking Authentication Chain",
     "description" : "The authentication chain that will be executed when a user is required to be
authenticated locally to match their user account with that of a remotely authenticated assertion.",
     "propertyOrder" : 500,
     "required" : true,
     "type" : "string",
     "exampleValue" : ""
   },
   "authenticationLevel" : {
     "title" : "Authentication Level",
     "description" : "The authentication level associated with this module.<br><br>Each
authentication module has an authentication level that can be used to indicate the level of security
associated with the module; 0 is the lowest (and the default).",
     "propertyOrder" : 100,
     "required" : true,
     "type" : "integer",
     "exampleValue" : ""
   },
   "isPassive" : {
     "title" : "Passive Authentication",
     "description" : "Use this parameter to indicate whether the identity provider should
authenticate passively (true) or not (false).",
     "propertyOrder" : 1200,
     "required" : true,
     "type" : "string",
     "exampleValue" : ""
   },
   "binding" : {
     "title" : "Response Binding",
     "description" : "Use this parameter to indicate what binding the IdP should use when
communicating with this SP.",
```

```
      "propertyOrder" : 1000,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
```

Global Operations

Resource path: `/global-config/authentication/modules/authSaml`

Resource version: `1.0`

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action Saml2Module --global --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action Saml2Module --global --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action Saml2Module --global --actionName nextdescendents
```

read

Usage:

```
am> read Saml2Module --global
```

update

Usage:

```
am> update Saml2Module --global --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "defaults" : {
      "properties" : {
        "nameIdFormat" : {
          "title" : "NameID Format",
          "description" : "(Optional) Use this parameter to specify a SAML Name
 Identifier format identifier such as <pre>urn:oasis:names:tc:SAML:2.0:nameid-
format:persistent</pre> <pre>urn:oasis:names:tc:SAML:2.0:nameid-format:transient</pre>
 <pre>urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified</pre>",
          "propertyOrder" : 1300,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "sloEnabled" : {
          "title" : "Single Logout Enabled",
          "description" : "Enable to attempt logout of the
 user's IdP session at the point of session logout. Required the
 <pre>org.forgerock.openam.authentication.modules.saml2.SAML2PostAuthenticationPlugin</pre> to be
 active on the chain that includes this SAML2 module.",
          "propertyOrder" : 1400,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "forceAuthn" : {
          "title" : "Force IdP Authentication",
          "description" : "Use this parameter to indicate whether the identity provider should force
 authentication (true) or can reuse existing security contexts (false).",
          "propertyOrder" : 1100,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "metaAlias" : {
          "title" : "SP MetaAlias",
          "description" : "MetaAlias for Service Provider. The format of this parameter is <pre>/
realm_name/SP</pre>",
          "propertyOrder" : 300,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "entityName" : {
          "title" : "IdP Entity ID",
          "description" : "The entity name of the SAML2 IdP Service to use for this module (must be
 configured).",
          "propertyOrder" : 200,
```

```
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "authComparison" : {
          "title" : "Comparison Type",
          "description" : "(Optional) Use this parameter to specify a comparison method to evaluate
the requested context classes or statements. OpenAM accepts the following values: <pre>better</pre>,
<pre>exact</pre>, <pre>maximum</pre>, and <pre>minimum</pre>.",
          "propertyOrder" : 600,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "reqBinding" : {
          "title" : "Request Binding",
          "description" : "Use this parameter to indicate what binding the SP should use when
communicating with the IdP.",
          "propertyOrder" : 900,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "sloRelay" : {
          "title" : "Single Logout URL",
          "description" : "If Single Logout is enabled, this is the URL to which the user should be
forwarded after successful IdP logout. This must be a fully-qualified URL (start with http...), or
the redirect will not function.",
          "propertyOrder" : 1500,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "loginChain" : {
          "title" : "Linking Authentication Chain",
          "description" : "The authentication chain that will be executed when a user is required
to be authenticated locally to match their user account with that of a remotely authenticated
assertion.",
          "propertyOrder" : 500,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "binding" : {
          "title" : "Response Binding",
          "description" : "Use this parameter to indicate what binding the IdP should use when
communicating with this SP.",
          "propertyOrder" : 1000,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "isPassive" : {
          "title" : "Passive Authentication",
          "description" : "Use this parameter to indicate whether the identity provider should
authenticate passively (true) or not (false).",
          "propertyOrder" : 1200,
          "required" : true,
          "type" : "string",
```

```
          "exampleValue" : ""
        },
        "authnContextDeclRef" : {
          "title" : "Authentication Context Declaration Reference",
          "description" : "(Optional) Use this parameter to specify authentication context declaration
 references. Separate multiple values with pipe characters (|).",
          "propertyOrder" : 800,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "authenticationLevel" : {
          "title" : "Authentication Level",
          "description" : "The authentication level associated with this module.<br><br>Each
 authentication module has an authentication level that can be used to indicate the level of security
 associated with the module; 0 is the lowest (and the default).",
          "propertyOrder" : 100,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "authnContextClassRef" : {
          "title" : "Authentication Context Class Reference",
          "description" : "(Optional) Use this parameter to specify authentication context class
 references. Separate multiple values with pipe characters (|).",
          "propertyOrder" : 700,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "allowCreate" : {
          "title" : "Allow IdP to Create NameID",
          "description" : "Use this parameter to indicate whether the identity provider can create a
 new identifier for the principal if none exists (true) or not (false).",
          "propertyOrder" : 400,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      },
      "type" : "object",
      "title" : "Realm Defaults"
    }
  }
}
```


SamlV2ServiceConfiguration

Global Operations

Resource path: `/global-config/services/saml2`

Resource version: `1.0`

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action SamlV2ServiceConfiguration --global --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action SamlV2ServiceConfiguration --global --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action SamlV2ServiceConfiguration --global --actionName nextdescendents
```

read

Usage:

```
am> read SamlV2ServiceConfiguration --global
```

update

Usage:

```
am> update SamlV2ServiceConfiguration --global --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "xmlEncryptionClass" : {
      "title" : "XML Encryption SPI implementation class",
      "description" : "Used by the SAML2 engine to <em>encrypt</em> and <em>decrypt</em> documents.",
      "propertyOrder" : 700,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
```

```
    },
    "bufferLength" : {
      "title" : "Buffer length (in bytes) to decompress request",
      "description" : "Specify the size of the buffer used for decompressing requests, in bytes.",
      "propertyOrder" : 1300,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "idpDiscoveryCookieDomain" : {
      "title" : "Cookie domain for IdP Discovery Service",
      "description" : "Specifies the cookie domain for the IDP discovery service.",
      "propertyOrder" : 400,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "nameIDInfoAttribute" : {
      "title" : "Attribute name for Name ID information",
      "description" : "User entry attribute to store name identifier information.",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "nameIDInfoKeyAttribute" : {
      "title" : "Attribute name for Name ID information key",
      "description" : "User entry attribute to store the name identifier key.",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "signingCertValidation" : {
      "title" : "XML Signing Certificate Validation",
      "description" : "If enabled, then validate certificates used to sign documents.",
      "propertyOrder" : 1000,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "encryptedKeyInKeyInfo" : {
      "title" : "Include xenc:EncryptedKey inside ds:KeyInfo Element",
      "description" : "Specify whether to include the <code>xenc:EncryptedKey</code> property inside
the <code>ds:KeyInfo</code> element.",
      "propertyOrder" : 800,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "xmlSigningClass" : {
      "title" : "XML Signing SPI implementation class",
      "description" : "Used by the SAML2 engine to <em>sign</em> documents.",
      "propertyOrder" : 900,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "caCertValidation" : {
```

```
      "title" : "CA Certificate Validation",
      "description" : "If enabled, then validate CA certificates.",
      "propertyOrder" : 1100,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "cacheCleanupInterval" : {
      "title" : "Cache cleanup interval (in seconds)",
      "description" : "Time between cache cleanup operations, in seconds.",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "idpDiscoveryUrlSchema" : {
      "title" : "URL scheme for IdP Discovery Service",
      "description" : "Specifies the URL scheme to use.",
      "propertyOrder" : 600,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "idpDiscoveryCookieType" : {
      "title" : "Cookie type for IdP Discovery Service",
      "description" : "Specifies the cookie type to use.",
      "propertyOrder" : 500,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
```

SamlV2SoapBinding

Global Operations

Resource path: `/global-config/services/federation/saml2soapbinding`

Resource version: `1.0`

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action SamlV2SoapBinding --global --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action SamlV2SoapBinding --global --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action SamlV2SoapBinding --global --actionName nextdescendents
```

read

Usage:

```
am> read SamlV2SoapBinding --global
```

update

Usage:

```
am> update SamlV2SoapBinding --global --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "requestHandlers" : {
      "title" : "Request Handler List",
      "description" : "List of handlers to deal with SAML v2.0 requests bound to SOAP. <p><p>The
 required format is: <code>key=<em>Meta Alias</em>|class=<em>Handler Class</em></code> <p><p>Set
 the <em>key</em> property for a request handler to the meta alias, and the <em>class</em>
 property to the name of the class that implements the handler.<p><p> For example: <code>key=/pdp|
class=com.sun.identity.xacml.plugins.XACMLAuthzDecisionQueryHandler</code>",
      "propertyOrder" : 100,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    }
  }
}
```

ScriptStore

Realm Operations

Resource path: `/realm-config/services/scripts`

Resource version: `1.0`

create

Usage:

```
am> create ScriptStore --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "lastModifiedDate" : {
      "title" : "Last modification date",
```

```
     "description" : "A string containing the last modified date and time, in ISO 8601 format. If
the script has not been modified since it was created, this property will have the same value as
creationDate",
     "propertyOrder" : 1000,
     "required" : true,
     "type" : "string",
     "exampleValue" : ""
   },
   "language" : {
     "title" : "Script language",
     "description" : "The language the script is written in - JAVASCRIPT or GROOVY",
     "propertyOrder" : 1000,
     "required" : true,
     "type" : "string",
     "exampleValue" : ""
   },
   "script" : {
     "title" : "Script",
     "description" : "The source code of the script. The source code is in UTF-8 format and encoded
into Base64",
     "propertyOrder" : 1000,
     "required" : true,
     "type" : "string",
     "exampleValue" : ""
   },
   "createdBy" : {
     "title" : "Created by",
     "description" : "A string containing the universal identifier DN of the subject that created the
script",
     "propertyOrder" : 1000,
     "required" : true,
     "type" : "string",
     "exampleValue" : ""
   },
   "lastModifiedBy" : {
     "title" : "Last modifier",
     "description" : "A string containing the universal identifier DN of the subject that most
recently updated the script. If the script has not been modified since it was created, this property
will have the same value as createdBy",
     "propertyOrder" : 1000,
     "required" : true,
     "type" : "string",
     "exampleValue" : ""
   },
   "name" : {
     "title" : "Script name",
     "description" : "The name provided for the script",
     "propertyOrder" : 1000,
     "required" : true,
     "type" : "string",
     "exampleValue" : ""
   },
   "description" : {
     "title" : "Script description",
     "description" : "An optional text string to help identify the script",
     "propertyOrder" : 1000,
     "required" : true,
     "type" : "string",
     "exampleValue" : ""
```

```
    },
    "creationDate" : {
      "title" : "Creation date",
      "description" : "An integer containing the creation date and time, in ISO 8601 format",
      "propertyOrder" : 1000,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "context" : {
      "title" : "Script type",
      "description" : "The script type. Supported values are: POLICY_CONDITION : Policy Condition
 AUTHENTICATION_SERVER_SIDE : Server-side Authentication  AUTHENTICATION_CLIENT_SIDE : Client-side
 Authentication - Note Client-side scripts must be written in JavaScript OIDC_CLAIMS : OIDC Claims
 SOCIAL_IDP_PROFILE_TRANSFORMATION : Social Identity Provider Profile Transformation",
      "propertyOrder" : 1000,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
```

delete

Usage:

```
am> delete ScriptStore --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action ScriptStore --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action ScriptStore --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action ScriptStore --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query ScriptStore --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read ScriptStore --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update ScriptStore --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "lastModifiedDate" : {
      "title" : "Last modification date",
      "description" : "A string containing the last modified date and time, in ISO 8601 format. If
 the script has not been modified since it was created, this property will have the same value as
 creationDate",
      "propertyOrder" : 1000,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "language" : {
      "title" : "Script language",
      "description" : "The language the script is written in - JAVASCRIPT or GROOVY",
      "propertyOrder" : 1000,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "script" : {
      "title" : "Script",
      "description" : "The source code of the script. The source code is in UTF-8 format and encoded
 into Base64",
      "propertyOrder" : 1000,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "createdBy" : {
      "title" : "Created by",
      "description" : "A string containing the universal identifier DN of the subject that created the
 script",
      "propertyOrder" : 1000,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "lastModifiedBy" : {
      "title" : "Last modifier",
      "description" : "A string containing the universal identifier DN of the subject that most
 recently updated the script. If the script has not been modified since it was created, this property
 will have the same value as createdBy",
      "propertyOrder" : 1000,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "name" : {
      "title" : "Script name",
      "description" : "The name provided for the script",
      "propertyOrder" : 1000,
      "required" : true,
      "type" : "string",
```

```
      "exampleValue" : ""
    },
    "description" : {
      "title" : "Script description",
      "description" : "An optional text string to help identify the script",
      "propertyOrder" : 1000,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "creationDate" : {
      "title" : "Creation date",
      "description" : "An integer containing the creation date and time, in ISO 8601 format",
      "propertyOrder" : 1000,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "context" : {
      "title" : "Script type",
      "description" : "The script type. Supported values are: POLICY_CONDITION : Policy Condition
 AUTHENTICATION_SERVER_SIDE : Server-side Authentication  AUTHENTICATION_CLIENT_SIDE : Client-side
 Authentication - Note Client-side scripts must be written in JavaScript OIDC_CLAIMS : OIDC Claims
 SOCIAL_IDP_PROFILE_TRANSFORMATION : Social Identity Provider Profile Transformation",
      "propertyOrder" : 1000,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
```

ScriptTypes

Global Operations

Resource path: `/global-config/services/scripting/contexts`

Resource version: `1.0`

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action ScriptTypes --global --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action ScriptTypes --global --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action ScriptTypes --global --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query ScriptTypes --global --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read ScriptTypes --global --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update ScriptTypes --global --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "defaultScript" : {
      "title" : "Default Script",
      "description" : "The source code that is presented as the default when creating a new script of
 this type.",
      "propertyOrder" : 1200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "languages" : {
      "title" : "Scripting languages",
      "description" : "The language the script is written in.<br><br>This is used to determine how to
 validate the script, as well as which engine to run the script within.",
      "propertyOrder" : 1100,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    }
  }
}
```

ScriptedDecision

Realm Operations

Resource path: `/realm-config/authentication/authenticationtrees/nodes/ScriptedDecisionNode`

Resource version: `1.0`

create

Usage:

```
am> create ScriptedDecision --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "outcomes" : {
      "title" : "Outcomes",
      "description" : "",
      "propertyOrder" : 200,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "inputs" : {
      "title" : "Script Inputs",
      "description" : "A list of state inputs required by the script.",
      "propertyOrder" : 300,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "script" : {
      "title" : "Script",
      "description" : "The script to evaluate.",
      "propertyOrder" : 100,
      "type" : "string",
      "exampleValue" : ""
    },
    "outputs" : {
      "title" : "Script Outputs",
      "description" : "A list of state outputs produced by the script.",
      "propertyOrder" : 400,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    }
  },
  "required" : [ "script", "outputs", "inputs", "outcomes" ]
}
```

delete

Usage:

```
am> delete ScriptedDecision --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action ScriptedDecision --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action ScriptedDecision --realm Realm --actionName getCreatableTypes
```

listOutcomes

List the available outcomes for the node type.

Usage:

```
am> action ScriptedDecision --realm Realm --body body --actionName listOutcomes
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "title" : "Some configuration of the node. This does not need to be complete against the
 configuration schema."
}
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action ScriptedDecision --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query ScriptedDecision --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read ScriptedDecision --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update ScriptedDecision --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "outcomes" : {
      "title" : "Outcomes",
```

```
      "description" : "",
      "propertyOrder" : 200,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "inputs" : {
      "title" : "Script Inputs",
      "description" : "A list of state inputs required by the script.",
      "propertyOrder" : 300,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "script" : {
      "title" : "Script",
      "description" : "The script to evaluate.",
      "propertyOrder" : 100,
      "type" : "string",
      "exampleValue" : ""
    },
    "outputs" : {
      "title" : "Script Outputs",
      "description" : "A list of state outputs produced by the script.",
      "propertyOrder" : 400,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    }
  },
  "required" : [ "script", "outputs", "inputs", "outcomes" ]
}
```

ScriptedModule

Realm Operations

Resource path: `/realm-config/authentication/modules/scripted`

Resource version: `1.0`

create

Usage:

```
am> create ScriptedModule --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "clientScript" : {
      "title" : "Client-side Script",
      "description" : "The client-side script.",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "authenticationLevel" : {
      "title" : "Authentication Level",
      "description" : "The authentication level associated with the authentication module.<br><br>Each
 authentication module has an authentication level that can be used to indicate the level of security
 associated with the module; 0 is the lowest (and the default).",
      "propertyOrder" : 400,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "clientScriptEnabled" : {
      "title" : "Client-side Script Enabled",
      "description" : "Enable this setting if the client-side script should be executed.",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "serverScript" : {
      "title" : "Server-side Script",
      "description" : "The server-side script to execute.<br><br>This script will be run on the
 server, subsequent to any client script having returned.",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
```

delete

Usage:

```
am> delete ScriptedModule --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action ScriptedModule --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action ScriptedModule --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action ScriptedModule --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query ScriptedModule --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read ScriptedModule --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update ScriptedModule --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "clientScript" : {
      "title" : "Client-side Script",
      "description" : "The client-side script.",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "authenticationLevel" : {
      "title" : "Authentication Level",
      "description" : "The authentication level associated with the authentication module.<br><br>Each
 authentication module has an authentication level that can be used to indicate the level of security
 associated with the module; 0 is the lowest (and the default).",
      "propertyOrder" : 400,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "clientScriptEnabled" : {
      "title" : "Client-side Script Enabled",
      "description" : "Enable this setting if the client-side script should be executed.",
      "propertyOrder" : 100,
```

```
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "serverScript" : {
      "title" : "Server-side Script",
      "description" : "The server-side script to execute.<br><br>This script will be run on the
 server, subsequent to any client script having returned.",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
```

Global Operations

Resource path: `/global-config/authentication/modules/scripted`

Resource version: `1.0`

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action ScriptedModule --global --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action ScriptedModule --global --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action ScriptedModule --global --actionName nextdescendents
```

read

Usage:

```
am> read ScriptedModule --global
```

update

Usage:

```
am> update ScriptedModule --global --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "defaults" : {
      "properties" : {
        "clientScript" : {
          "title" : "Client-side Script",
          "description" : "The client-side script.",
          "propertyOrder" : 200,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "serverScript" : {
          "title" : "Server-side Script",
          "description" : "The server-side script to execute.<br><br>This script will be run on the
 server, subsequent to any client script having returned.",
          "propertyOrder" : 300,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "authenticationLevel" : {
          "title" : "Authentication Level",
          "description" : "The authentication level associated with the authentication
 module.<br><br>Each authentication module has an authentication level that can be used to indicate
 the level of security associated with the module; 0 is the lowest (and the default).",
          "propertyOrder" : 400,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "clientScriptEnabled" : {
          "title" : "Client-side Script Enabled",
          "description" : "Enable this setting if the client-side script should be executed.",
          "propertyOrder" : 100,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
```

```
        }
      },
      "type" : "object",
      "title" : "Realm Defaults"
    }
  }
}
```

Scripting

Global Operations

Resource path: `/global-config/services/scripting`

Resource version: `1.0`

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action Scripting --global --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action Scripting --global --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action Scripting --global --actionName nextdescendents
```

read

Usage:

```
am> read Scripting --global
```

update

Usage:

```
am> update Scripting --global --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "defaultContext" : {
      "title" : "Default Script Type",
      "description" : "The default script context type when creating a new script.",
      "propertyOrder" : 900,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
```

ScriptingEngineConfiguration

Global Operations

Resource path: `/global-config/services/scripting/contexts/{contexts}/engineConfiguration`

Resource version: `1.0`

create

Usage:

```
am> create ScriptingEngineConfiguration --global --contexts contexts --body body
```

Parameters:

--contexts

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "idleTimeout" : {
      "title" : "Thread idle timeout (seconds)",
      "description" : "Length of time (in seconds) to wait before terminating threads.<br><br>Length
of time (in seconds) to wait before terminating threads that were started when the queue reached
capacity. Only applies to threads beyond the core pool size (up to the maximum size).",
      "propertyOrder" : 500,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "serverTimeout" : {
      "title" : "Server-side Script Timeout",
      "description" : "The maximum execution time any individual script should take on the server (in
seconds).<br><br>Server-side scripts will be forcibly stopped after this amount of execution time.",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "useSecurityManager" : {
      "title" : "Use system SecurityManager",
      "description" : "Indicates whether the system SecurityManager should also be consulted when
checking access to Java classes.<br><br>If enabled, then the checkPackageAccess method will be called
for each Java class accessed. If no SecurityManager is configured, then this has no effect.",
      "propertyOrder" : 800,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "blackList" : {
      "title" : "Java class blacklist",
      "description" : "List of patterns of Java classes that must not be accessed by a
script.<br><br>This blacklist is applied after the whitelist to apply additional restrictions. For
instance you may whitelist java.lang.* and then blacklist java.lang.System and java.lang.Runtime. It
is recommended to always prefer specific whitelists where possible.",
      "propertyOrder" : 700,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "maxThreads" : {
      "title" : "Maximum thread pool size",
      "description" : "The maximum size of the thread pool from which scripts will operate.<br><br>New
threads will be created up to this size once the task queue reaches capacity. Has no effect if the
queue is unbounded.",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
```

```
    },
    "coreThreads" : {
      "title" : "Core thread pool size",
      "description" : "The core size of the thread pool from which scripts will operate.",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "whiteList" : {
      "title" : "Java class whitelist",
      "description" : "List of patterns of allowed Java classes that may be loaded/accessed by
 scripts.<br><br>Each Java class accessed by a script must match at least one of these patterns. Use
 '*' as a wildcard, e.g. <code>java.lang.*</code>",
      "propertyOrder" : 600,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "queueSize" : {
      "title" : "Thread pool queue size",
      "description" : "Size of queue to use for buffering script execution request when core pool is
 at capacity.<br><br>Use -1 for an unbounded queue (this disables the maximum pool size setting). For
 short, CPU-bound scripts, consider a small pool size and larger queue length. For I/O-bound scripts
 (e.g., REST calls) consider a larger maximum pool size and a smaller queue. Not hot-swappable:
 restart server for changes to take effect.",
      "propertyOrder" : 400,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    }
  }
}
```

delete

Usage:

```
am> delete ScriptingEngineConfiguration --global --contexts contexts
```

Parameters:

--contexts

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action ScriptingEngineConfiguration --global --contexts contexts --actionName getAllTypes
```

Parameters:

--contexts

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action ScriptingEngineConfiguration --global --contexts contexts --actionName getCreatableTypes
```

Parameters:

--contexts

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action ScriptingEngineConfiguration --global --contexts contexts --actionName nextdescendents
```

Parameters:

--contexts

read

Usage:

```
am> read ScriptingEngineConfiguration --global --contexts contexts
```

Parameters:

--contexts

update

Usage:

```
am> update ScriptingEngineConfiguration --global --contexts contexts --body body
```

Parameters:

--contexts

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "idleTimeout" : {
      "title" : "Thread idle timeout (seconds)",
      "description" : "Length of time (in seconds) to wait before terminating threads.<br><br>Length
 of time (in seconds) to wait before terminating threads that were started when the queue reached
 capacity. Only applies to threads beyond the core pool size (up to the maximum size).",
      "propertyOrder" : 500,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "serverTimeout" : {
      "title" : "Server-side Script Timeout",
      "description" : "The maximum execution time any individual script should take on the server (in
 seconds).<br><br>Server-side scripts will be forcibly stopped after this amount of execution time.",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "useSecurityManager" : {
      "title" : "Use system SecurityManager",
      "description" : "Indicates whether the system SecurityManager should also be consulted when
 checking access to Java classes.<br><br>If enabled, then the checkPackageAccess method will be called
 for each Java class accessed. If no SecurityManager is configured, then this has no effect.",
      "propertyOrder" : 800,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "blackList" : {
      "title" : "Java class blacklist",
      "description" : "List of patterns of Java classes that must not be accessed by a
 script.<br><br>This blacklist is applied after the whitelist to apply additional restrictions. For
 instance you may whitelist java.lang.* and then blacklist java.lang.System and java.lang.Runtime. It
 is recommended to always prefer specific whitelists where possible.",
      "propertyOrder" : 700,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "maxThreads" : {
      "title" : "Maximum thread pool size",
      "description" : "The maximum size of the thread pool from which scripts will operate.<br><br>New
 threads will be created up to this size once the task queue reaches capacity. Has no effect if the
 queue is unbounded.",
```

```
      "propertyOrder" : 300,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "coreThreads" : {
      "title" : "Core thread pool size",
      "description" : "The core size of the thread pool from which scripts will operate.",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "whiteList" : {
      "title" : "Java class whitelist",
      "description" : "List of patterns of allowed Java classes that may be loaded/accessed by
 scripts.<br><br>Each Java class accessed by a script must match at least one of these patterns. Use
 '*' as a wildcard, e.g. <code>java.lang.*</code>",
      "propertyOrder" : 600,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "queueSize" : {
      "title" : "Thread pool queue size",
      "description" : "Size of queue to use for buffering script execution request when core pool is
 at capacity.<br><br>Use -1 for an unbounded queue (this disables the maximum pool size setting). For
 short, CPU-bound scripts, consider a small pool size and larger queue length. For I/O-bound scripts
 (e.g., REST calls) consider a larger maximum pool size and a smaller queue. Not hot-swappable:
 restart server for changes to take effect.",
      "propertyOrder" : 400,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    }
  }
}
```

Scripts

Realm Operations

The script resources service is responsible for managing scripts used for client-side and server-side scripted authentication, custom policy conditions, and handling OpenID Connect claims. Scripts are represented in JSON and take the following form. Scripts are built from standard JSON objects and values (strings, numbers, objects, sets, arrays, true, false, and null). Each script has a system-generated universally unique identifier (UUID), which must be used when modifying existing scripts. Renaming a script will not affect the UUID

Resource path: `/scripts`

Resource version: `1.1`

create

Create a script in a realm. The value for script must be in UTF-8 format and then encoded into Base64.

Usage:

```
am> create Scripts --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "description" : "Script resource endpoint json schema",
  "type" : "object",
  "title" : "Script resource schema",
  "properties" : {
    "_id" : {
      "title" : "Script unique ID",
      "description" : "A unique ID for a script configuration, provided by the server",
      "type" : "string"
    },
    "name" : {
      "title" : "Script name",
      "description" : "The name provided for the script",
      "type" : "string"
    },
    "description" : {
      "title" : "Script description",
      "description" : "An optional text string to help identify the script",
      "type" : "string"
    },
    "script" : {
      "title" : "Script",
      "description" : "The source code of the script. The source code is in UTF-8 format and encoded
 into Base64",
      "type" : "string"
    },
    "language" : {
      "title" : "Script language",
      "description" : "The language the script is written in - JAVASCRIPT or GROOVY",
      "type" : "string"
    },
    "context" : {
      "title" : "Script type",
      "description" : "The script type. Supported values are: POLICY_CONDITION : Policy Condition
 AUTHENTICATION_SERVER_SIDE : Server-side Authentication  AUTHENTICATION_CLIENT_SIDE : Client-side
 Authentication - Note Client-side scripts must be written in JavaScript OIDC_CLAIMS : OIDC Claims",
```

```
      "type" : "string"
    },
    "createdBy" : {
      "title" : "Created by",
      "description" : "A string containing the universal identifier DN of the subject that created the
 script",
      "type" : "string"
    },
    "creationDate" : {
      "title" : "Creation date",
      "description" : "An integer containing the creation date and time, in ISO 8601 format",
      "type" : "number"
    },
    "lastModifiedBy" : {
      "title" : "Last modifier",
      "description" : "A string containing the universal identifier DN of the subject that most
 recently updated the script. If the script has not been modified since it was created, this property
 will have the same value as createdBy",
      "type" : "string"
    },
    "lastModifiedDate" : {
      "title" : "Last modification date",
      "description" : "A string containing the last modified date and time, in ISO 8601 format. If
 the script has not been modified since it was created, this property will have the same value as
 creationDate",
      "type" : "number"
    }
  },
  "required" : [ "name", "description", "script", "language", "context" ]
}
```

delete

Delete an individual script in a realm specified by the UUID parameter

Usage:

```
am> delete Scripts --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

query

List all the scripts in a realm, as well as any global scripts

Usage:

```
am> query Scripts --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all. Fields that can be queried: [*]

read

Read an individual script in a realm by specifying the UUID parameter

Usage:

```
am> read Scripts --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Update an individual script in a realm specified by the UUID parameter

Usage:

```
am> update Scripts --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "description" : "Script resource endpoint json schema",
  "type" : "object",
  "title" : "Script resource schema",
  "properties" : {
    "_id" : {
      "title" : "Script unique ID",
      "description" : "A unique ID for a script configuration, provided by the server",
      "type" : "string"
    },
    "name" : {
      "title" : "Script name",
      "description" : "The name provided for the script",
      "type" : "string"
    },
    "description" : {
      "title" : "Script description",
      "description" : "An optional text string to help identify the script",
      "type" : "string"
    },
```

```
    "script" : {
      "title" : "Script",
      "description" : "The source code of the script. The source code is in UTF-8 format and encoded
 into Base64",
      "type" : "string"
    },
    "language" : {
      "title" : "Script language",
      "description" : "The language the script is written in - JAVASCRIPT or GROOVY",
      "type" : "string"
    },
    "context" : {
      "title" : "Script type",
      "description" : "The script type. Supported values are: POLICY_CONDITION : Policy Condition
 AUTHENTICATION_SERVER_SIDE : Server-side Authentication  AUTHENTICATION_CLIENT_SIDE : Client-side
 Authentication - Note Client-side scripts must be written in JavaScript OIDC_CLAIMS : OIDC Claims",
      "type" : "string"
    },
    "createdBy" : {
      "title" : "Created by",
      "description" : "A string containing the universal identifier DN of the subject that created the
 script",
      "type" : "string"
    },
    "creationDate" : {
      "title" : "Creation date",
      "description" : "An integer containing the creation date and time, in ISO 8601 format",
      "type" : "number"
    },
    "lastModifiedBy" : {
      "title" : "Last modifier",
      "description" : "A string containing the universal identifier DN of the subject that most
 recently updated the script. If the script has not been modified since it was created, this property
 will have the same value as createdBy",
      "type" : "string"
    },
    "lastModifiedDate" : {
      "title" : "Last modification date",
      "description" : "A string containing the last modified date and time, in ISO 8601 format. If
 the script has not been modified since it was created, this property will have the same value as
 creationDate",
      "type" : "number"
    }
  },
  "required" : [ "name", "description", "script", "language", "context" ]
}
```

validate

Validate a script. Include a JSON representation of the script and the script language, JAVASCRIPT or GROOVY, in the POST data. The value for script must be in UTF-8 format and then encoded into Base64

Usage:

```
am> action Scripts --realm Realm --body body --actionName validate
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "description" : "Validate action request schema",
  "type" : "object",
  "title" : "Validate request schema",
  "properties" : {
    "script" : {
      "title" : "Script",
      "description" : "The source code of the script. The source code is in UTF-8 format and encoded
 into Base64",
      "type" : "string"
    },
    "language" : {
      "title" : "Script language",
      "description" : "The language the script is written in - JAVASCRIPT or GROOVY",
      "type" : "string"
    }
  },
  "required" : [ "script", "language" ]
}
```

SdkProperties

Global Operations

An object of property key-value pairs

Resource path: `/global-config/servers/{serverName}/properties/sdk`

Resource version: `1.0`

read

Usage:

```
am> read SdkProperties --global --serverName serverName
```

Parameters:

--serverName

An object of property key-value pairs

update

Usage:

```
am> update SdkProperties --global --serverName serverName --body body
```

Parameters:

--serverName

An object of property key-value pairs

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "amconfig.header.datastore" : {
      "title" : "Data Store",
      "type" : "object",
      "propertyOrder" : 0,
      "properties" : {
        "com.sun.identity.sm.enableDataStoreNotification" : {
          "title" : "Enable Datastore Notification",
          "type" : "object",
          "propertyOrder" : 0,
          "description" : "Specifies if backend datastore notification is enabled. If
 this value is set to 'false', then in-memory notification is enabled. (property name:
 com.sun.identity.sm.enableDataStoreNotification)",
          "properties" : {
            "value" : {
              "type" : "boolean",
              "required" : false
            },
            "inherited" : {
              "type" : "boolean",
              "required" : true
            }
          }
        },
        "com.sun.identity.sm.notification.threadpool.size" : {
          "title" : "Notification Pool Size",
          "type" : "object",
          "propertyOrder" : 1,
          "description" : "Specifies the size of the sm notification thread pool (total number of
 threads). (property name: com.sun.identity.sm.notification.threadpool.size)",
          "properties" : {
            "value" : {
              "type" : "integer",
              "required" : false
            },
            "inherited" : {
              "type" : "boolean",
              "required" : true
            }
          }
        }
      }
    },
```

```
   "amconfig.header.eventservice" : {
     "title" : "Event Service",
     "type" : "object",
     "propertyOrder" : 1,
     "properties" : {
       "com.iplanet.am.event.connection.num.retries" : {
         "title" : "Number of retries for Event Service connections",
         "type" : "object",
         "propertyOrder" : 0,
         "description" : "Specifies the number of attempts made to successfully re-establish the
Event Service connections. (property name: com.iplanet.am.event.connection.num.retries)",
         "properties" : {
           "value" : {
             "type" : "integer",
             "required" : false
           },
           "inherited" : {
             "type" : "boolean",
             "required" : true
           }
         }
       },
       "com.iplanet.am.event.connection.delay.between.retries" : {
         "title" : "Delay between Event Service connection retries",
         "type" : "object",
         "propertyOrder" : 1,
         "description" : "Specifies the delay in milliseconds between retries to re-establish the
Event Service connections. (property name: com.iplanet.am.event.connection.delay.between.retries)",
         "properties" : {
           "value" : {
             "type" : "integer",
             "required" : false
           },
           "inherited" : {
             "type" : "boolean",
             "required" : true
           }
         }
       },
       "com.iplanet.am.event.connection.ldap.error.codes.retries" : {
         "title" : "Error codes for Event Service connection retries",
         "type" : "object",
         "propertyOrder" : 2,
         "description" : "This secifies the LDAP exception error codes for which
retries to re-establish Event Service connections will trigger. (property name:
com.iplanet.am.event.connection.ldap.error.codes.retries)",
         "properties" : {
           "value" : {
             "type" : "string",
             "required" : false
           },
           "inherited" : {
             "type" : "boolean",
             "required" : true
           }
         }
       },
       "com.sun.am.event.connection.disable.list" : {
         "title" : "Disabled Event Service Connection",
```

```
          "type" : "object",
          "propertyOrder" : 3,
          "description" : "Specifies which event connection (persistent search) to be disabled. There
are three valid values - aci, sm and um (case insensitive). Multiple values should be separated with
\",\". (property name: com.sun.am.event.connection.disable.list)",
          "properties" : {
            "value" : {
              "type" : "string",
              "required" : false
            },
            "inherited" : {
              "type" : "boolean",
              "required" : true
            }
          }
        }
      }
    },
    "amconfig.header.ldapconnection" : {
      "title" : "LDAP Connection",
      "type" : "object",
      "propertyOrder" : 2,
      "properties" : {
        "com.iplanet.am.ldap.connection.num.retries" : {
          "title" : "Number of retries for LDAP Connection",
          "type" : "object",
          "propertyOrder" : 0,
          "description" : "Specifies the number of attempts made to successfully re-establish LDAP
Connection. (property name: com.iplanet.am.ldap.connection.num.retries)",
          "properties" : {
            "value" : {
              "type" : "integer",
              "required" : false
            },
            "inherited" : {
              "type" : "boolean",
              "required" : true
            }
          }
        },
        "com.iplanet.am.ldap.connection.delay.between.retries" : {
          "title" : "Delay between LDAP connection retries",
          "type" : "object",
          "propertyOrder" : 1,
          "description" : "Specifies the delay in milliseconds between retries to re-establish the
LDAP connections. (property name: com.iplanet.am.ldap.connection.delay.between.retries)",
          "properties" : {
            "value" : {
              "type" : "integer",
              "required" : false
            },
            "inherited" : {
              "type" : "boolean",
              "required" : true
            }
          }
        },
        "com.iplanet.am.ldap.connection.ldap.error.codes.retries" : {
          "title" : "Error codes for LDAP connection retries",
```

```
          "type" : "object",
          "propertyOrder" : 2,
          "description" : "This secifies the LDAP exception error codes for
which retries to re-establish LDAP connections will trigger. (property name:
com.iplanet.am.ldap.connection.ldap.error.codes.retries)",
          "properties" : {
            "value" : {
              "type" : "string",
              "required" : false
            },
            "inherited" : {
              "type" : "boolean",
              "required" : true
            }
          }
        }
      }
    },
    "amconfig.header.cachingreplica" : {
      "title" : "Caching and Replica",
      "type" : "object",
      "propertyOrder" : 3,
      "properties" : {
        "com.iplanet.am.sdk.cache.maxSize" : {
          "title" : "SDK Caching Max. Size",
          "type" : "object",
          "propertyOrder" : 0,
          "description" : "Specifies the size of the cache when SDK caching is enabled. The size
should be an integer greater than 0, or default size (10000) will be used. Changing this value will
reset (clear) the contents of the cache. (property name: com.iplanet.am.sdk.cache.maxSize)",
          "properties" : {
            "value" : {
              "type" : "integer",
              "required" : false
            },
            "inherited" : {
              "type" : "boolean",
              "required" : true
            }
          }
        }
      }
    },
    "amconfig.header.sdktimetoliveconfig" : {
      "title" : "Time To Live Configuration",
      "type" : "object",
      "propertyOrder" : 4,
      "properties" : {
        "com.iplanet.am.sdk.cache.entry.expire.enabled" : {
          "title" : "Cache Entry Expiration Enabled",
          "type" : "object",
          "propertyOrder" : 0,
          "description" : "If this property is set, the cache entries will expire
based on the time specified in User Entry Expiration Time property. (property name:
com.iplanet.am.sdk.cache.entry.expire.enabled)",
          "properties" : {
            "value" : {
              "type" : "boolean",
              "required" : false
```

```
            },
            "inherited" : {
              "type" : "boolean",
              "required" : true
            }
          }
        },
        "com.iplanet.am.sdk.cache.entry.user.expire.time" : {
          "title" : "User Entry Expiration Time",
          "type" : "object",
          "propertyOrder" : 1,
          "description" : "This property specifies time in minutes for which the user entries remain
 valid in cache after their last modification. After this specified period of time elapses (after the
 last modification/read from the directory), the data for the entry that is cached will expire. At
 that instant new requests for data for these user entries will result in reading from the Directory.
 (property name: com.iplanet.am.sdk.cache.entry.user.expire.time)",
          "properties" : {
            "value" : {
              "type" : "integer",
              "required" : false
            },
            "inherited" : {
              "type" : "boolean",
              "required" : true
            }
          }
        },
        "com.iplanet.am.sdk.cache.entry.default.expire.time" : {
          "title" : "Default Entry Expiration Time",
          "type" : "object",
          "propertyOrder" : 2,
          "description" : "This property specifies time in minutes for which the non-user entries
 remain valid in cache after their last modification. After this specified period of time elapses
 (after the last modification/read from the directory), the data for the entry that is cached will
 expire. At that instant new requests for data for these non-user entries will result in reading from
 the Directory. (property name: com.iplanet.am.sdk.cache.entry.default.expire.time)",
          "properties" : {
            "value" : {
              "type" : "integer",
              "required" : false
            },
            "inherited" : {
              "type" : "boolean",
              "required" : true
            }
          }
        }
      }
    }
  }
}
```

SecretStores

Realm Operations

Services that provide sources of secret values

Resource path: `/realm-config/secrets/stores`

Resource version: `1.0`

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action SecretStores --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action SecretStores --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action SecretStores --realm Realm --actionName nextdescendents
```

Global Operations

Services that provide sources of secret values

Resource path: `/global-config/secrets/stores`

Resource version: `1.0`

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action SecretStores --global --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action SecretStores --global --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action SecretStores --global --actionName nextdescendents
```

Secrets

Realm Operations

Secrets represent cryptographic values such as private keys

Resource path: `/realm-config/secrets`

Resource version: `1.0`

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action Secrets --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action Secrets --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action Secrets --realm Realm --actionName nextdescendents
```

Global Operations

Secrets represent cryptographic values such as private keys

Resource path: `/global-config/secrets`

Resource version: `1.0`

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action Secrets --global --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action Secrets --global --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action Secrets --global --actionName nextdescendents
```

SecurID

Realm Operations

Resource path: `/realm-config/authentication/modules/securid`

Resource version: `1.0`

create

Usage:

```
am> create SecurID --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "serverConfigPath" : {
      "title" : "ACE/Server Configuration Path",
      "description" : "The path to the ACE/Server configuration files",
      "propertyOrder" : null,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "authenticationLevel" : {
      "title" : "Authentication Level",
      "description" : "The authentication level associated with this module.<br><br>Each
 authentication module has an authentication level that can be used to indicate the level of security
 associated with the module; 0 is the lowest (and the default). ",
      "propertyOrder" : null,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    }
  }
}
```

delete

Usage:

```
am> delete SecurID --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action SecurID --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action SecurID --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action SecurID --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query SecurID --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read SecurID --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update SecurID --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "serverConfigPath" : {
      "title" : "ACE/Server Configuration Path",
      "description" : "The path to the ACE/Server configuration files",
      "propertyOrder" : null,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "authenticationLevel" : {
      "title" : "Authentication Level",
      "description" : "The authentication level associated with this module.<br><br>Each
 authentication module has an authentication level that can be used to indicate the level of security
 associated with the module; 0 is the lowest (and the default). ",
      "propertyOrder" : null,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    }
  }
}
```

Global Operations

Resource path: `/global-config/authentication/modules/securid`

Resource version: `1.0`

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action SecurID --global --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action SecurID --global --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action SecurID --global --actionName nextdescendents
```

read

Usage:

```
am> read SecurID --global
```

update

Usage:

```
am> update SecurID --global --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "defaults" : {
      "properties" : {
        "authenticationLevel" : {
          "title" : "Authentication Level",
          "description" : "The authentication level associated with this module.<br><br>Each
 authentication module has an authentication level that can be used to indicate the level of security
 associated with the module; 0 is the lowest (and the default). ",
          "propertyOrder" : null,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "serverConfigPath" : {
          "title" : "ACE/Server Configuration Path",
          "description" : "The path to the ACE/Server configuration files",
          "propertyOrder" : null,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      },
      "type" : "object",
      "title" : "Realm Defaults"
    }
  }
}
```


SecurityProperties

Global Operations

An object of property key-value pairs

Resource path: `/global-config/servers/{serverName}/properties/security`

Resource version: `1.0`

read

Usage:

```
am> read SecurityProperties --global --serverName serverName
```

Parameters:

`--serverName`

An object of property key-value pairs

update

Usage:

```
am> update SecurityProperties --global --serverName serverName --body body
```

Parameters:

--serverName

An object of property key-value pairs

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "amconfig.header.encryption" : {
      "title" : "Encryption",
      "type" : "object",
      "propertyOrder" : 0,
      "properties" : {
        "am.encryption.pwd" : {
          "title" : "Password Encryption Key",
          "type" : "object",
          "propertyOrder" : 0,
          "description" : "The encryption key value for decrypting passwords stored in the Service
 Management System configuration. (property name: am.encryption.pwd)",
          "properties" : {
            "value" : {
              "type" : "string",
              "required" : false
            },
            "inherited" : {
              "type" : "boolean",
              "required" : true
            }
          }
        },
        "com.iplanet.security.encryptor" : {
          "title" : "Encryption class",
          "type" : "object",
          "propertyOrder" : 1,
          "description" : "The default encryption class. (property name:
 com.iplanet.security.encryptor)",
          "properties" : {
            "value" : {
              "type" : "string",
              "required" : false
            },
            "inherited" : {
              "type" : "boolean",
              "required" : true
            }
          }
        },
```

```
       "com.iplanet.security.SecureRandomFactoryImpl" : {
         "title" : "Secure Random Factory Class",
         "type" : "object",
         "propertyOrder" : 2,
         "description" : "This property is used for specifying SecureRandomFactory class. Available
values for this property are com.iplanet.am.util.JSSSecureRandomFactoryImpl that is using JSS
and com.iplanet.am.util.SecureRandomFactoryImpl that is using pure Java only. (property name:
com.iplanet.security.SecureRandomFactoryImpl)",
         "properties" : {
           "value" : {
             "type" : "string",
             "required" : false
           },
           "inherited" : {
             "type" : "boolean",
             "required" : true
           }
         }
       }
     }
   },
   "amconfig.header.validation" : {
     "title" : "Validation",
     "type" : "object",
     "propertyOrder" : 1,
     "properties" : {
       "com.iplanet.services.comm.server.pllrequest.maxContentLength" : {
         "title" : "Platform Low Level Comm. Max. Content Length",
         "type" : "object",
         "propertyOrder" : 0,
         "description" : "Maximum content-length for an HttpRequest. (property name:
com.iplanet.services.comm.server.pllrequest.maxContentLength)",
         "properties" : {
           "value" : {
             "type" : "integer",
             "required" : false
           },
           "inherited" : {
             "type" : "boolean",
             "required" : true
           }
         }
       },
       "com.iplanet.am.clientIPCheckEnabled" : {
         "title" : "Client IP Address Check",
         "type" : "object",
         "propertyOrder" : 1,
         "description" : "Specifies whether or not the IP address of the client is checked in all
single sign on token creations or validations. (property name: com.iplanet.am.clientIPCheckEnabled)",
         "properties" : {
           "value" : {
             "type" : "boolean",
             "required" : false
           },
           "inherited" : {
             "type" : "boolean",
             "required" : true
           }
         }
```

```
        }
      }
    },
    "amconfig.header.cookie" : {
      "title" : "Cookie",
      "type" : "object",
      "propertyOrder" : 2,
      "properties" : {
        "com.iplanet.am.cookie.name" : {
          "title" : "Cookie Name",
          "type" : "object",
          "propertyOrder" : 0,
          "description" : "The cookie name used by Authentication Service to set the valid
session handler ID. This name is used to retrieve the valid session information. (property name:
com.iplanet.am.cookie.name)",
          "properties" : {
            "value" : {
              "type" : "string",
              "required" : false
            },
            "inherited" : {
              "type" : "boolean",
              "required" : true
            }
          }
        },
        "com.iplanet.am.cookie.secure" : {
          "title" : "Secure Cookie",
          "type" : "object",
          "propertyOrder" : 1,
          "description" : "Specifies whether to set cookie in a secure mode in which the browser
will only return the cookie when a secure protocol such as HTTP(s) is used. (property name:
com.iplanet.am.cookie.secure)",
          "properties" : {
            "value" : {
              "type" : "boolean",
              "required" : false
            },
            "inherited" : {
              "type" : "boolean",
              "required" : true
            }
          }
        },
        "com.iplanet.am.cookie.encode" : {
          "title" : "Encode Cookie Value",
          "type" : "object",
          "propertyOrder" : 2,
          "description" : "Specifies whether to URL encode the cookie value. (property name:
com.iplanet.am.cookie.encode)",
          "properties" : {
            "value" : {
              "type" : "boolean",
              "required" : false
            },
            "inherited" : {
              "type" : "boolean",
              "required" : true
            }
```

```
          }
        }
      }
    },
    "amconfig.header.securitykey" : {
      "title" : "Key Store",
      "type" : "object",
      "propertyOrder" : 3,
      "properties" : {
        "com.sun.identity.saml.xmlsig.keystore" : {
          "title" : "Keystore File",
          "type" : "object",
          "propertyOrder" : 0,
          "description" : "Specifies the location of the keystore file. (property name:
com.sun.identity.saml.xmlsig.keystore)",
          "properties" : {
            "value" : {
              "type" : "string",
              "required" : false
            },
            "inherited" : {
              "type" : "boolean",
              "required" : true
            }
          }
        },
        "com.sun.identity.saml.xmlsig.storetype" : {
          "title" : "Keystore Type",
          "type" : "object",
          "propertyOrder" : 1,
          "description" : "Specifies the keystore type. (property name:
com.sun.identity.saml.xmlsig.storetype)",
          "properties" : {
            "value" : {
              "type" : "string",
              "required" : false
            },
            "inherited" : {
              "type" : "boolean",
              "required" : true
            }
          }
        },
        "com.sun.identity.saml.xmlsig.storepass" : {
          "title" : "Keystore Password File",
          "type" : "object",
          "propertyOrder" : 2,
          "description" : "Specifies the location of the file that contains the password used to
access the keystore file. (property name: com.sun.identity.saml.xmlsig.storepass)",
          "properties" : {
            "value" : {
              "type" : "string",
              "required" : false
            },
            "inherited" : {
              "type" : "boolean",
              "required" : true
            }
          }
```

```
      },
      "com.sun.identity.saml.xmlsig.keypass" : {
        "title" : "Private Key Password File",
        "type" : "object",
        "propertyOrder" : 3,
        "description" : "Specifies the location of the file that contains the
password used to protect the private key of a generated key pair. (property name:
com.sun.identity.saml.xmlsig.keypass)",
        "properties" : {
          "value" : {
            "type" : "string",
            "required" : false
          },
          "inherited" : {
            "type" : "boolean",
            "required" : true
          }
        }
      },
      "com.sun.identity.saml.xmlsig.certalias" : {
        "title" : "Certificate Alias",
        "type" : "object",
        "propertyOrder" : 4,
        "description" : "(property name: com.sun.identity.saml.xmlsig.certalias)",
        "properties" : {
          "value" : {
            "type" : "string",
            "required" : false
          },
          "inherited" : {
            "type" : "boolean",
            "required" : true
          }
        }
      }
    }
  },
  "amconfig.header.crlcache" : {
    "title" : "Certificate Revocation List Caching",
    "type" : "object",
    "propertyOrder" : 4,
    "properties" : {
      "com.sun.identity.crl.cache.directory.host" : {
        "title" : "LDAP server host name",
        "type" : "object",
        "propertyOrder" : 0,
        "description" : "",
        "properties" : {
          "value" : {
            "type" : "string",
            "required" : false
          },
          "inherited" : {
            "type" : "boolean",
            "required" : true
          }
        }
      },
      "com.sun.identity.crl.cache.directory.port" : {
```

```
          "title" : "LDAP server port number",
          "type" : "object",
          "propertyOrder" : 1,
          "description" : "",
          "properties" : {
            "value" : {
              "type" : "integer",
              "required" : false
            },
            "inherited" : {
              "type" : "boolean",
              "required" : true
            }
          }
        },
        "com.sun.identity.crl.cache.directory.ssl" : {
          "title" : "SSL/TLS Enabled",
          "type" : "object",
          "propertyOrder" : 2,
          "description" : "",
          "properties" : {
            "value" : {
              "type" : "boolean",
              "required" : false
            },
            "inherited" : {
              "type" : "boolean",
              "required" : true
            }
          }
        },
        "com.sun.identity.crl.cache.directory.user" : {
          "title" : "LDAP server bind user name",
          "type" : "object",
          "propertyOrder" : 3,
          "description" : "",
          "properties" : {
            "value" : {
              "type" : "string",
              "required" : false
            },
            "inherited" : {
              "type" : "boolean",
              "required" : true
            }
          }
        },
        "com.sun.identity.crl.cache.directory.password" : {
          "title" : "LDAP server bind password",
          "type" : "object",
          "propertyOrder" : 4,
          "description" : "",
          "properties" : {
            "value" : {
              "type" : "string",
              "required" : false,
              "format" : "password"
            },
            "inherited" : {
```

```
              "type" : "boolean",
              "required" : true
            }
          }
        },
        "com.sun.identity.crl.cache.directory.searchlocs" : {
          "title" : "LDAP search base DN",
          "type" : "object",
          "propertyOrder" : 5,
          "description" : "",
          "properties" : {
            "value" : {
              "type" : "string",
              "required" : false
            },
            "inherited" : {
              "type" : "boolean",
              "required" : true
            }
          }
        },
        "com.sun.identity.crl.cache.directory.searchattr" : {
          "title" : "Search Attributes",
          "type" : "object",
          "propertyOrder" : 6,
          "description" : "Any DN component of issuer's subjectDN can be used to retrieve CRL from
local LDAP server. It is single value string, like, \"cn\". All Root CA need to use the same search
attribute.",
          "properties" : {
            "value" : {
              "type" : "string",
              "required" : false
            },
            "inherited" : {
              "type" : "boolean",
              "required" : true
            }
          }
        }
      }
    },
    "amconfig.header.ocsp.check" : {
      "title" : "Online Certificate Status Protocol Check",
      "type" : "object",
      "propertyOrder" : 5,
      "properties" : {
        "com.sun.identity.authentication.ocspCheck" : {
          "title" : "Check Enabled",
          "type" : "object",
          "propertyOrder" : 0,
          "description" : "",
          "properties" : {
            "value" : {
              "type" : "boolean",
              "required" : false
            },
            "inherited" : {
              "type" : "boolean",
              "required" : true
```

```
            }
          }
        },
        "com.sun.identity.authentication.ocsp.responder.url" : {
          "title" : "Responder URL",
          "type" : "object",
          "propertyOrder" : 1,
          "description" : "",
          "properties" : {
            "value" : {
              "type" : "string",
              "required" : false
            },
            "inherited" : {
              "type" : "boolean",
              "required" : true
            }
          }
        },
        "com.sun.identity.authentication.ocsp.responder.nickname" : {
          "title" : "Certificate Nickname",
          "type" : "object",
          "propertyOrder" : 2,
          "description" : "",
          "properties" : {
            "value" : {
              "type" : "string",
              "required" : false
            },
            "inherited" : {
              "type" : "boolean",
              "required" : true
            }
          }
        }
      }
    },
    "amconfig.header.deserialisationwhitelist" : {
      "title" : "Object Deserialisation Class Whitelist",
      "type" : "object",
      "propertyOrder" : 6,
      "properties" : {
        "openam.deserialisation.classes.whitelist" : {
          "title" : "Whitelist",
          "type" : "object",
          "propertyOrder" : 0,
          "description" : "The list of classes that are considered valid when OpenAM performs
Object deserialisation operations. The defaults should work for most installations. (property name:
openam.deserialisation.classes.whitelist)",
          "properties" : {
            "value" : {
              "type" : "string",
              "required" : false
            },
            "inherited" : {
              "type" : "boolean",
              "required" : true
            }
          }
```

```
        }
      }
    }
  }
}
```

SecurityTokenServices

Realm Operations

Security Token Services configuration

Resource path: `/realm-config/services/sts`

Resource version: `1.0`

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action SecurityTokenServices --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action SecurityTokenServices --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action SecurityTokenServices --realm Realm --actionName nextdescendents
```

SelectIdentityProvider

Realm Operations

Resource path: `/realm-config/authentication/authenticationtrees/nodes/SelectIdPNode`

Resource version: `1.0`

create

Usage:

```
am> create SelectIdentityProvider --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "passwordAttribute" : {
      "title" : "Password attribute",
      "description" : "The attribute in the user object that verifies that user during local
 authentication.",
      "propertyOrder" : 300,
      "type" : "string",
      "exampleValue" : ""
    },
    "includeLocalAuthentication" : {
      "title" : "Include local authentication",
      "description" : "Whether local authentication will be included as an available identity
 provider.",
      "propertyOrder" : 100,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "identityAttribute" : {
      "title" : "Identity Attribute",
      "description" : "The attribute used to retrieve an existing user. Required to support the offer
 of only existing providers.",
      "propertyOrder" : 500,
      "type" : "string",
      "exampleValue" : ""
    },
    "offerOnlyExisting" : {
      "title" : "Offer only existing providers",
      "description" : "Choices offered should be limited to those already associated with a user
 object.",
      "propertyOrder" : 200,
      "type" : "boolean",
      "exampleValue" : ""
```

```
    }
  },
  "required" : [ "offerOnlyExisting", "identityAttribute", "includeLocalAuthentication",
 "passwordAttribute" ]
}
```

delete

Usage:

```
am> delete SelectIdentityProvider --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action SelectIdentityProvider --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action SelectIdentityProvider --realm Realm --actionName getCreatableTypes
```

listOutcomes

List the available outcomes for the node type.

Usage:

```
am> action SelectIdentityProvider --realm Realm --body body --actionName listOutcomes
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "title" : "Some configuration of the node. This does not need to be complete against the
 configuration schema."
}
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action SelectIdentityProvider --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query SelectIdentityProvider --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read SelectIdentityProvider --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update SelectIdentityProvider --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "passwordAttribute" : {
      "title" : "Password attribute",
      "description" : "The attribute in the user object that verifies that user during local
 authentication.",
      "propertyOrder" : 300,
      "type" : "string",
      "exampleValue" : ""
    },
    "includeLocalAuthentication" : {
      "title" : "Include local authentication",
      "description" : "Whether local authentication will be included as an available identity
 provider.",
      "propertyOrder" : 100,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "identityAttribute" : {
      "title" : "Identity Attribute",
      "description" : "The attribute used to retrieve an existing user. Required to support the offer
 of only existing providers.",
      "propertyOrder" : 500,
      "type" : "string",
      "exampleValue" : ""
    },
    "offerOnlyExisting" : {
      "title" : "Offer only existing providers",
      "description" : "Choices offered should be limited to those already associated with a user
 object.",
      "propertyOrder" : 200,
      "type" : "boolean",
      "exampleValue" : ""
    }
  },
  "required" : [ "offerOnlyExisting", "identityAttribute", "includeLocalAuthentication",
 "passwordAttribute" ]
}
```

SelfServiceTreeConfig

Realm Operations

Resource path: `/realm-config/services/selfServiceTrees`

Resource version: `1.0`

create

Usage:

```
am> create SelfServiceTreeConfig --realm Realm --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "treeMapping" : {
      "title" : "Tree Mapping",
      "description" : "Maps the self service function name (the key) to an Authentication Tree (the
 value).",
      "propertyOrder" : 100,
      "required" : true,
      "patternProperties" : {
        ".*" : {
          "type" : "string"
        }
      },
      "type" : "object",
      "exampleValue" : ""
    },
    "enabled" : {
      "title" : "Enabled",
      "description" : "",
      "propertyOrder" : 90,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    }
  }
}
```

delete

Usage:

```
am> delete SelfServiceTreeConfig --realm Realm
```

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action SelfServiceTreeConfig --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action SelfServiceTreeConfig --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action SelfServiceTreeConfig --realm Realm --actionName nextdescendents
```

read

Usage:

```
am> read SelfServiceTreeConfig --realm Realm
```

update

Usage:

```
am> update SelfServiceTreeConfig --realm Realm --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "treeMapping" : {
      "title" : "Tree Mapping",
      "description" : "Maps the self service function name (the key) to an Authentication Tree (the
 value).",
      "propertyOrder" : 100,
      "required" : true,
      "patternProperties" : {
        ".*" : {
          "type" : "string"
        }
      },
      "type" : "object",
      "exampleValue" : ""
    },
    "enabled" : {
      "title" : "Enabled",
      "description" : "",
      "propertyOrder" : 90,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    }
  }
}
```

SelfServiceTrees

Realm Operations

Self Service Tree resource contains a mapping between self service and authentication trees.

Resource path: `/selfservice/trees`

Resource version: `1.0`

read

Read the configured tree mapping.

Usage:

```
am> read SelfServiceTrees --realm Realm
```

Global Operations

Resource path: `/global-config/services/selfServiceTrees`

Resource version: `1.0`

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action SelfServiceTrees --global --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action SelfServiceTrees --global --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action SelfServiceTrees --global --actionName nextdescendents
```

read

Usage:

```
am> read SelfServiceTrees --global
```

update

Usage:

```
am> update SelfServiceTrees --global --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
```

```
  "properties" : {
    "defaults" : {
      "properties" : {
        "enabled" : {
          "title" : "Enabled",
          "description" : "",
          "propertyOrder" : 90,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "treeMapping" : {
          "title" : "Tree Mapping",
          "description" : "Maps the self service function name (the key) to an Authentication Tree
 (the value).",
          "propertyOrder" : 100,
          "required" : true,
          "patternProperties" : {
            ".*" : {
              "type" : "string"
            }
          },
          "type" : "object",
          "exampleValue" : ""
        }
      },
      "type" : "object",
      "title" : "Realm Defaults"
    }
  }
}
```

ServerInformation

Realm Operations

Provides information about the server.

Resource path: `/serverinfo`

Resource version: `1.1`

read

Read the server information.

Usage:

```
am> read ServerInformation --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

ServerVersion

Realm Operations

Server Version schema

Resource path: `/serverinfo/version`

Resource version: `1.0`

read

It returns information about OpenAM such as: version, revision and date

Usage:

```
am> read ServerVersion --realm Realm
```

Servers

Global Operations

Servers resource provider is responsible for managing Servers and their configuration for an OpenAM instance.

Resource path: `/global-config/servers`

Resource version: `1.0`

clone

Clone the specified Server, keeping it's settings but using a different URL.

Usage:

```
am> action Servers --global --body body --actionName clone
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "$schema" : "http://json-schema.org/draft-04/schema#",
  "description" : "Container for required data to clone a Server.",
  "type" : "object",
  "title" : "Clone Server Request schema",
  "properties" : {
    "clonedUrl" : {
      "type" : "string",
      "title" : "Cloned Server URL",
      "description" : "The new URL of the cloned server. Must be unique."
    }
  }
}
```

create

Create a Server.

Usage:

```
am> create Servers --global --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "$schema" : "http://json-schema.org/draft-04/schema#",
  "description" : "Describes the data that a Server Resource could contain.",
  "type" : "object",
  "title" : "Server resource schema",
  "properties" : {
    "_id" : {
      "type" : "string",
      "title" : "Server id",
      "description" : "Unique identifier of the Server."
    },
    "siteName" : {
      "type" : "string",
      "title" : "Site name",
      "description" : "The Server's name."
    },
    "url" : {
      "type" : "string",
      "title" : "Url",
      "description" : "The URL of the Server."
    }
  }
}
```

delete

Delete a Server.

Usage:

```
am> delete Servers --global --id id
```

Parameters:

--id

The unique identifier for the resource.

query

Query the collection of the Servers.

Usage:

```
am> query Servers --global --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all. Fields that can be queried: [*]

read

Read a Server.

Usage:

```
am> read Servers --global --id id
```

Parameters:

--id

The unique identifier for the resource.

Services

Realm Operations

The collection of services available on a realm.

Resource path: `/realm-config/services`

Resource version: `1.0`

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action Services --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action Services --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action Services --realm Realm --actionName nextdescendents
```

query

Find services provisioned for the realm - query for a particular service by identifier, or request all services using `_queryFilter=true`

Usage:

```
am> query Services --realm Realm --filter filter
```

Parameters:

`--filter`

A CREST formatted query filter, where "true" will query all. Fields that can be queried: [_id]

Global Operations

Global and default configuration for services

Resource path: `/global-config/services`

Resource version: `1.0`

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action Services --global --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action Services --global --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action Services --global --actionName nextdescendents
```

Session

Realm Operations

Resource path: `/realm-config/services/session`

Resource version: `1.0`

create

Usage:

```
am> create Session --realm Realm --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
```

```
   "dynamic" : {
     "properties" : {
       "maxSessionTime" : {
         "title" : "Maximum Session Time",
         "description" : "Maximum time a session can remain valid before OpenAM requires the user to
 authenticate again, in minutes.",
         "propertyOrder" : 100,
         "required" : true,
         "type" : "integer",
         "exampleValue" : ""
       },
       "maxIdleTime" : {
         "title" : "Maximum Idle Time",
         "description" : "Maximum time a CTS-based session can remain idle before OpenAM requires the
 user to authenticate again, in minutes.",
         "propertyOrder" : 200,
         "required" : true,
         "type" : "integer",
         "exampleValue" : ""
       },
       "quotaLimit" : {
         "title" : "Active User Sessions",
         "description" : "Maximum number of concurrent CTS-based sessions OpenAM allows a user to
 have.",
         "propertyOrder" : 800,
         "required" : true,
         "type" : "integer",
         "exampleValue" : ""
       },
       "maxCachingTime" : {
         "title" : "Maximum Caching Time",
         "description" : "Maximum time that external clients of AM are recommended to cache the
 session for, in minutes.",
         "propertyOrder" : 300,
         "required" : true,
         "type" : "integer",
         "exampleValue" : ""
       }
     },
     "type" : "object",
     "title" : "Dynamic Attributes"
   }
 }
}
```

delete

Usage:

```
am> delete Session --realm Realm
```

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action Session --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action Session --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action Session --realm Realm --actionName nextdescendents
```

read

Usage:

```
am> read Session --realm Realm
```

update

Usage:

```
am> update Session --realm Realm --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "dynamic" : {
      "properties" : {
        "maxSessionTime" : {
          "title" : "Maximum Session Time",
          "description" : "Maximum time a session can remain valid before OpenAM requires the user to
 authenticate again, in minutes.",
          "propertyOrder" : 100,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
```

```
        "maxIdleTime" : {
          "title" : "Maximum Idle Time",
          "description" : "Maximum time a CTS-based session can remain idle before OpenAM requires the
 user to authenticate again, in minutes.",
          "propertyOrder" : 200,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "quotaLimit" : {
          "title" : "Active User Sessions",
          "description" : "Maximum number of concurrent CTS-based sessions OpenAM allows a user to
 have.",
          "propertyOrder" : 800,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "maxCachingTime" : {
          "title" : "Maximum Caching Time",
          "description" : "Maximum time that external clients of AM are recommended to cache the
 session for, in minutes.",
          "propertyOrder" : 300,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        }
      },
      "type" : "object",
      "title" : "Dynamic Attributes"
    }
  }
}
```

Global Operations

Resource path: `/global-config/services/session`

Resource version: `1.0`

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action Session --global --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action Session --global --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action Session --global --actionName nextdescendents
```

read

Usage:

```
am> read Session --global
```

update

Usage:

```
am> update Session --global --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "stateless" : {
      "type" : "object",
      "title" : "Client-based Sessions",
      "propertyOrder" : 4,
      "properties" : {
        "statelessCompressionType" : {
          "title" : "Compression Algorithm",
          "description" : "If enabled the session state is compressed before signing and
 encryption.<br><br><strong>WARNING</strong>: Enabling compression may compromise encryption. This may
 leak information about the content of the session state if encryption is enabled.",
          "propertyOrder" : 2500,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "statelessSigningType" : {
          "title" : "Signing Algorithm Type",
          "description" : "Specifies the algorithm that AM uses to sign the JSON Web Token
 (JWT) containing the session content. Signing the JWT enables tampering detection.<br><br>AM
 supports the following signing algorithms: <ul><li><strong>HS256</strong>. HMAC using SHA-256.</
li><li><strong>HS384</strong>. HMAC using SHA-384.</li><li><strong>HS512</strong>. HMAC using
 SHA-512.</li><li><strong>RS256</strong>. RSASSA-PKCS1-v1_5 using SHA-256.</li><li><strong>ES256</
```

```
strong>. ECDSA using SHA-256 and NIST standard P-256 elliptic curve.</li><li><strong>ES384</strong>.
 ECDSA using SHA-384 and NIST standard P-384 elliptic curve.</li><li><strong>ES512</strong>. ECDSA
 using SHA-512 and NIST standard P-521 elliptic curve.</li></ul>",
          "propertyOrder" : 1900,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "openam-session-stateless-blacklist-poll-interval" : {
          "title" : "Blacklist Poll Interval (seconds)",
          "description" : "Specifies the interval at which AM polls the Core Token Service to update
 the list of logged out sessions, in seconds.<br><br>The longer the polling interval, the more
 time a malicious user has to connect to other AM servers in a deployment and make use of a stolen
 session cookie. Shortening the polling interval improves the security for logged out sessions, but
 might incur a minimal decrease in overall AM performance due to increased network activity. Set to
 <code>0</code> to disable this feature completely.",
          "propertyOrder" : 2800,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "openam-session-stateless-blacklist-cache-size" : {
          "title" : "Session Blacklist Cache Size",
          "description" : "Number of blacklisted sessions to cache in memory to speed up blacklist
 checks and reduce load on the CTS. The cache size should be approximately the number of logouts
 expected in the maximum session time.",
          "propertyOrder" : 2700,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "statelessSigningRsaCertAlias" : {
          "title" : "Signing RSA/ECDSA Certificate Alias",
          "description" : "Specify the alias of a certificate containing a public/private key
 pair that AM uses when performing RSA or ECDSA signing on the session JWT. Specify a signing
 certificate alias when using a \"Signing Algorithm Type\" of <code>RS256</code>, <code>ES256</code>,
 <code>ES384</code>, or <code>ES512</code>.<br><br>The certificate is retrieved from the keystore
 specified by the <code>com.sun.identity.saml.xmlsig.keystore</code> property.",
          "propertyOrder" : 2100,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "statelessEncryptionType" : {
          "title" : "Encryption Algorithm",
          "description" : "Specifies the algorithm that AM uses to encrypt the JSON Web
 Token (JWT) containing the session content.<br><br>AM supports the following encryption
 algorithms:<ul><li><strong>NONE</strong>. No encryption is selected.</li><li><strong>RSA</
strong>. Session content is encrypted with AES using a unique key. The key is then encrypted
 with an RSA public key and appended to the JWT.<p><p>AM supports the following padding modes,
 which you can set using the <code>org.forgerock.openam.session.stateless.rsa.padding</code>
 advanced property:<ul><li><code>RSA1_5</code>. RSA with PKCS#1 v1.5 padding.</li><li><code>RSA-
OAEP</code>. RSA with optimal asymmetric encryption padding (OAEP) and SHA-1.</li><li><code>RSA-
OAEP-256</code>. RSA with OAEP padding and SHA-256.</li></ul></li><li><strong>AES KeyWrapping</
strong>. Session content is encrypted with AES using a unique key and is then wrapped using AES
 KeyWrap and the master key. This provides additional security, compared to RSA, at the cost
 of 128 or 256 bits (or 32 bytes) depending on the size of the master key. This method provides
 authenticated encryption, which removes the need for a separate signature and decreases the
 byte size of the JWT. See <a href=\"https://tools.ietf.org/html/rfc3394\" target=\"_blank\">RFC
```

```
 3394</a>.</li><li><strong>Direct AES Encryption</strong>.  Session content is encrypted with
 direct AES encryption with a symmetric key. This method provides authenticated encryption,
 which removes the need for a separate signature and decreases the byte size of the JWT. </li></
ul><p><p><strong>Important</strong>: To prevent users from accidentally disabling all authentication
 support, which can be accomplished by disabling signing and not using an authenticated encryption
 mode, you must set the <code>org.forgerock.openam.session.stateless.signing.allownone</code> system
 property to <code>true</code> to turn off signing completely.",
          "propertyOrder" : 2200,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "statelessEncryptionAesKey" : {
          "title" : "Encryption Symmetric AES Key",
          "description" : "AES key for use with Direct or AES KeyWrap encryption modes.<br><br>The
 symmetric AES key is a base64-encoded random key.<p><p>For direct encryption with <code>AES-GCM</
code> or for <code>AES-KeyWrap</code> with any content encryption method, this should be 128, 192, or
 256 bits.<p><p>For direct encryption with <code>AES-CBC-HMAC</code>, the key should be double those
 sizes (one half for the AES key, the other have for the HMAC key).<p><p>AES key sizes greater than
 128 bits require installation of the JCE Unlimited Strength policy files in your JRE.",
          "propertyOrder" : 2400,
          "required" : true,
          "type" : "string",
          "format" : "password",
          "exampleValue" : ""
        },
        "openam-session-stateless-enable-session-blacklisting" : {
          "title" : "Enable Session Blacklisting",
          "description" : "Blacklists client-based sessions that log out.<br><br>We recommend enabling
 this setting if the maximum session time is high. Blacklist state is stored in the Core Token Service
 (CTS) token store until the session expires, in order to ensure that sessions cannot continue to be
 used.",
          "propertyOrder" : 2600,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "openam-session-stateless-blacklist-purge-delay" : {
          "title" : "Blacklist Purge Delay (minutes)",
          "description" : "When added to the maximum session time, specifies the amount of time that
 AM tracks logged out sessions.<br><br>Increase the blacklist purge delay if you expect system clock
 skews in a deployment of AM servers to be greater than one minute. There is no need to increase the
 blacklist purge delay for servers running a clock synchronization protocol, such as Network Time
 Protocol.",
          "propertyOrder" : 2900,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "statelessEncryptionRsaCertAlias" : {
          "title" : "Encryption RSA Certificate Alias",
          "description" : "Specifies the alias of a certificate containing a public/private key pair
 that AM uses when encrypting a JWT. Specify an encryption certificate alias when using an Encryption
 Algorithm Type of <code>RSA</code>.<br><br>The certificate is retrieved from the keystore referenced
 by the <code>com.sun.identity.saml.xmlsig.keystore</code> property.",
          "propertyOrder" : 2300,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
```

```
       },
       "statelessSigningHmacSecret" : {
         "title" : "Signing HMAC Shared Secret",
         "description" : "Specifies the shared secret that AM uses when performing HMAC signing
on the session JWT.<p><p>Specify a shared secret when using a \"Signing Algorithm Type\" of
<code>HS256</code>, <code>HS384</code>, or <code>HS512</code>.",
         "propertyOrder" : 2000,
         "required" : true,
         "type" : "string",
         "format" : "password",
         "exampleValue" : ""
       }
     }
   },
   "general" : {
     "type" : "object",
     "title" : "General",
     "propertyOrder" : 0,
     "properties" : {
       "latestAccessTimeUpdateFrequency" : {
         "title" : "Latest Access Time Update Frequency",
         "description" : "Defaults to <code>60</code> seconds. At most, AM updates a session's
latest access time this often.<br><br>Subsequent touches to the session that occur within the
specified number of seconds after an update will not cause additional updates to the session's
access time.<p><p>Refreshing a session returns the idle time as the number of seconds since an
update has occurred, which will be between <code>0</code> and the specified Latest Access Time Update
Frequency.",
         "propertyOrder" : null,
         "required" : true,
         "type" : "integer",
         "exampleValue" : ""
       },
       "dnRestrictionOnly" : {
         "title" : "DN Restriction Only Enabled",
         "description" : "If enabled, OpenAM will not perform DNS lookups when checking restrictions
in cookie hijacking mode.",
         "propertyOrder" : 1300,
         "required" : true,
         "type" : "boolean",
         "exampleValue" : ""
       },
       "timeoutHandlers" : {
         "title" : "Session Timeout Handler implementations",
         "description" : "Lists plugin classes implementing session timeout handlers. Specify the
fully qualified name.",
         "propertyOrder" : 1800,
         "required" : true,
         "items" : {
           "type" : "string"
         },
         "type" : "array",
         "exampleValue" : ""
       }
     }
   },
   "notifications" : {
     "type" : "object",
     "title" : "Session Property Change Notifications",
     "propertyOrder" : 2,
```

```
     "properties" : {
       "notificationPropertyList" : {
         "title" : "Notification Properties",
         "description" : "Lists session properties for which OpenAM can send notifications upon
 modification. Session notification applies to CTS-based sessions only.",
         "propertyOrder" : 1200,
         "required" : true,
         "items" : {
           "type" : "string"
         },
         "type" : "array",
         "exampleValue" : ""
       },
       "propertyChangeNotifications" : {
         "title" : "Enable Property Change Notifications",
         "description" : "If on, then OpenAM notifies other applications participating in SSO when a
 session property in the Notification Properties list changes on a CTS-based session.",
         "propertyOrder" : 600,
         "required" : true,
         "type" : "string",
         "exampleValue" : ""
       }
     }
   },
   "quotas" : {
     "type" : "object",
     "title" : "Session Quotas",
     "propertyOrder" : 3,
     "properties" : {
       "denyLoginWhenRepoDown" : {
         "title" : "Deny user login when session repository is down",
         "description" : "This property only takes effect when the session quota constraint is
 enabled, and the session data store is unavailable.",
         "propertyOrder" : 1100,
         "required" : true,
         "type" : "string",
         "exampleValue" : ""
       },
       "behaviourWhenQuotaExhausted" : {
         "title" : "Resulting behavior if session quota exhausted",
         "description" : "Specify the action to take if a session quota is
 exhausted:<ul><li><strong>Deny Access</strong>. New session creation requests will be denied.</
li><li><strong>Destroy Next Expiring</strong>. The session that would expire next will be destroyed.</
li><li><strong>Destroy Oldest</strong>. The oldest session will be destroyed.</li><li><strong>Destroy
 All</strong>. All previous sessions will be destroyed.</li></ul>",
         "propertyOrder" : 1000,
         "required" : true,
         "type" : "string",
         "exampleValue" : ""
       },
       "iplanet-am-session-enable-session-constraint" : {
         "title" : "Enable Quota Constraints",
         "description" : "If on, then OpenAM allows you to set quota constraints on CTS-based
 sessions.",
         "propertyOrder" : 700,
         "required" : true,
         "type" : "string",
         "exampleValue" : ""
       },
```

```
       "quotaConstraintMaxWaitTime" : {
         "title" : "Read Timeout for Quota Constraint",
         "description" : "Maximum wait time after which OpenAM considers a search for live session
count as having failed if quota constraints are enabled, in milliseconds.",
         "propertyOrder" : 900,
         "required" : true,
         "type" : "integer",
         "exampleValue" : ""
       }
     }
   },
   "search" : {
     "type" : "object",
     "title" : "Session Search",
     "propertyOrder" : 1,
     "properties" : {
       "sessionListRetrievalTimeout" : {
         "title" : "Timeout for Search",
         "description" : "Time after which OpenAM sees an incomplete search as having failed, in
seconds.",
         "propertyOrder" : 500,
         "required" : true,
         "type" : "integer",
         "exampleValue" : ""
       },
       "maxSessionListSize" : {
         "title" : "Maximum Number of Search Results",
         "description" : "Maximum number of results from a session search. Do not set this attribute
to a large value, for example more than 1000, unless sufficient system resources are allocated.",
         "propertyOrder" : 400,
         "required" : true,
         "type" : "integer",
         "exampleValue" : ""
       }
     }
   },
   "dynamic" : {
     "properties" : {
       "maxSessionTime" : {
         "title" : "Maximum Session Time",
         "description" : "Maximum time a session can remain valid before OpenAM requires the user to
authenticate again, in minutes.",
         "propertyOrder" : 100,
         "required" : true,
         "type" : "integer",
         "exampleValue" : ""
       },
       "maxCachingTime" : {
         "title" : "Maximum Caching Time",
         "description" : "Maximum time that external clients of AM are recommended to cache the
session for, in minutes.",
         "propertyOrder" : 300,
         "required" : true,
         "type" : "integer",
         "exampleValue" : ""
       },
       "maxIdleTime" : {
         "title" : "Maximum Idle Time",
```

```
          "description" : "Maximum time a CTS-based session can remain idle before OpenAM requires the
 user to authenticate again, in minutes.",
          "propertyOrder" : 200,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "quotaLimit" : {
          "title" : "Active User Sessions",
          "description" : "Maximum number of concurrent CTS-based sessions OpenAM allows a user to
 have.",
          "propertyOrder" : 800,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        }
      },
      "type" : "object",
      "title" : "Dynamic Attributes"
    }
  }
}
```


SessionProperties

Global Operations

An object of property key-value pairs

Resource path: `/global-config/servers/{serverName}/properties/session`

Resource version: `1.0`

read

Usage:

```
am> read SessionProperties --global --serverName serverName
```

Parameters:

`--serverName`

An object of property key-value pairs

update

Usage:

```
am> update SessionProperties --global --serverName serverName --body body
```

Parameters:

--serverName

An object of property key-value pairs

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "amconfig.header.sessionthresholds" : {
      "title" : "Session Limits",
      "type" : "object",
      "propertyOrder" : 0,
      "properties" : {
        "org.forgerock.openam.session.service.access.persistence.caching.maxsize" : {
          "title" : "Maximum Session Cache Size",
          "type" : "object",
          "propertyOrder" : 0,
          "description" : "The maximum number of sessions to cache in the per-server internal session
 cache. (property name: org.forgerock.openam.session.service.access.persistence.caching.maxsize)",
          "properties" : {
            "value" : {
              "type" : "integer",
              "required" : false
            },
            "inherited" : {
              "type" : "boolean",
              "required" : true
            }
          }
        },
        "com.iplanet.am.session.invalidsessionmaxtime" : {
          "title" : "Invalidate Session Max Time",
          "type" : "object",
          "propertyOrder" : 1,
          "description" : "Duration in minutes after which the invalid session will be removed
 from the session table if it is created and the user does not login. This value should always
 be greater than the timeout value in the Authentication module properties file. (property name:
 com.iplanet.am.session.invalidsessionmaxtime)",
          "properties" : {
            "value" : {
              "type" : "integer",
              "required" : false
            },
            "inherited" : {
              "type" : "boolean",
              "required" : true
            }
          }
        }
      }
    },
```

```
   "amconfig.header.sessionlogging" : {
     "title" : "Statistics",
     "type" : "object",
     "propertyOrder" : 1,
     "properties" : {
       "com.iplanet.am.stats.interval" : {
         "title" : "Logging Interval (in seconds)",
         "type" : "object",
         "propertyOrder" : 0,
         "description" : "Number of seconds to elapse between statistics logging. The interval
should be at least 5 seconds to avoid CPU saturation. An interval value less than 5 seconds will be
interpreted as 5 seconds. (property name: com.iplanet.am.stats.interval)",
         "properties" : {
           "value" : {
             "type" : "integer",
             "required" : false
           },
           "inherited" : {
             "type" : "boolean",
             "required" : true
           }
         }
       },
       "com.iplanet.services.stats.state" : {
         "title" : "State",
         "type" : "object",
         "propertyOrder" : 1,
         "description" : "Statistics state 'file' will write to a file under the
specified directory, and 'console' will write into webserver log files. (property name:
com.iplanet.services.stats.state)",
         "properties" : {
           "value" : {
             "enum" : [ "off", "file", "console" ],
             "options" : {
               "enum_titles" : [ "Off", "File", "Console" ]
             },
             "type" : "string",
             "required" : false
           },
           "inherited" : {
             "type" : "boolean",
             "required" : true
           }
         }
       },
       "com.iplanet.services.stats.directory" : {
         "title" : "Directory",
         "type" : "object",
         "propertyOrder" : 2,
         "description" : "Directory where the statistic files will be created. Use forward slashes
\"/\" to separate directories, not backslash \"\\\". Spaces in the file name are allowed for Windows.
(property name: com.iplanet.services.stats.directory)",
         "properties" : {
           "value" : {
             "type" : "string",
             "required" : false
           },
           "inherited" : {
             "type" : "boolean",
```

```
              "required" : true
            }
          }
        },
        "com.sun.am.session.enableHostLookUp" : {
          "title" : "Enable Host Lookup",
          "type" : "object",
          "propertyOrder" : 3,
          "description" : "Enables or disables host lookup during session logging. (property name:
com.sun.am.session.enableHostLookUp)",
          "properties" : {
            "value" : {
              "type" : "boolean",
              "required" : false
            },
            "inherited" : {
              "type" : "boolean",
              "required" : true
            }
          }
        }
      }
    },
    "amconfig.header.sessionnotification" : {
      "title" : "Notification",
      "type" : "object",
      "propertyOrder" : 2,
      "properties" : {
        "com.iplanet.am.notification.threadpool.size" : {
          "title" : "Notification Pool Size",
          "type" : "object",
          "propertyOrder" : 0,
          "description" : "Specifies the size of the notification thread pool (total number of
threads). (property name: com.iplanet.am.notification.threadpool.size)",
          "properties" : {
            "value" : {
              "type" : "integer",
              "required" : false
            },
            "inherited" : {
              "type" : "boolean",
              "required" : true
            }
          }
        },
        "com.iplanet.am.notification.threadpool.threshold" : {
          "title" : "Notification Thread Pool Threshold",
          "type" : "object",
          "propertyOrder" : 1,
          "description" : "Specifies the maximum task queue length for serving notification threads.
(property name: com.iplanet.am.notification.threadpool.threshold)",
          "properties" : {
            "value" : {
              "type" : "integer",
              "required" : false
            },
            "inherited" : {
              "type" : "boolean",
              "required" : true
```

```
            }
          }
        }
      }
    },
    "amconfig.header.sessionvalidation" : {
      "title" : "Validation",
      "type" : "object",
      "propertyOrder" : 3,
      "properties" : {
        "com.sun.am.session.caseInsensitiveDN" : {
          "title" : "Case Insensitive client DN comparison",
          "type" : "object",
          "propertyOrder" : 0,
          "description" : "Specifies if client distinguished name comparison is case insensitive/
sensitive. (property name: com.sun.am.session.caseInsensitiveDN)",
          "properties" : {
            "value" : {
              "type" : "boolean",
              "required" : false
            },
            "inherited" : {
              "type" : "boolean",
              "required" : true
            }
          }
        }
      }
    }
  }
}
```

SessionPropertyWhiteList

Realm Operations

Resource path: `/realm-config/services/amSessionPropertyWhitelist`

Resource version: `1.0`

create

Usage:

```
am> create SessionPropertyWhiteList --realm Realm --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "whitelistedQueryProperties" : {
      "title" : "Session Properties to return for session queries",
      "description" : "A list of session properties that can be returned to admins in a REST session
 query response.<p><p>This setting may impact REST query performance - when session properties are
 added, the CTS token must be retrieved, and will be the subject of decryption and decompression, if
 configured.<p><p> Protected attributes will NOT be allowed to be set, edited or deleted, even if they
 are included in this list.",
      "propertyOrder" : 110,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "sessionPropertyWhitelist" : {
      "title" : "Whitelisted Session Property Names",
      "description" : "A list of properties that users may read, edit the value of, or delete from
 their session.<p><p> Adding properties to sessions can impact OpenAM's performance. Because there is
 no size constraint limiting the set of properties that you can add to sessions, and no limit on the
 number of session properties you can add, keep in mind that adding session properties can increase
 the load on an OpenAM deployment in the following areas: <ul><li>OpenAM server memory</li><li>OpenDJ
 storage</li><li>OpenDJ replication</li></ul><p>Protected attributes will NOT be allowed to be set,
 edited or deleted, even if they are included in this whitelist.",
      "propertyOrder" : 100,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    }
  }
}
```

delete

Usage:

```
am> delete SessionPropertyWhiteList --realm Realm
```

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action SessionPropertyWhiteList --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action SessionPropertyWhiteList --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action SessionPropertyWhiteList --realm Realm --actionName nextdescendents
```

read

Usage:

```
am> read SessionPropertyWhiteList --realm Realm
```

update

Usage:

```
am> update SessionPropertyWhiteList --realm Realm --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "whitelistedQueryProperties" : {
      "title" : "Session Properties to return for session queries",
      "description" : "A list of session properties that can be returned to admins in a REST session
 query response.<p><p>This setting may impact REST query performance - when session properties are
 added, the CTS token must be retrieved, and will be the subject of decryption and decompression, if
 configured.<p><p> Protected attributes will NOT be allowed to be set, edited or deleted, even if they
 are included in this list.",
      "propertyOrder" : 110,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "sessionPropertyWhitelist" : {
      "title" : "Whitelisted Session Property Names",
      "description" : "A list of properties that users may read, edit the value of, or delete from
 their session.<p><p> Adding properties to sessions can impact OpenAM's performance. Because there is
 no size constraint limiting the set of properties that you can add to sessions, and no limit on the
 number of session properties you can add, keep in mind that adding session properties can increase
 the load on an OpenAM deployment in the following areas: <ul><li>OpenAM server memory</li><li>OpenDJ
 storage</li><li>OpenDJ replication</li></ul><p>Protected attributes will NOT be allowed to be set,
 edited or deleted, even if they are included in this whitelist.",
      "propertyOrder" : 100,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    }
  }
}
```


Global Operations

Resource path: `/global-config/services/amSessionPropertyWhitelist`

Resource version: `1.0`

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action SessionPropertyWhiteList --global --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action SessionPropertyWhiteList --global --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action SessionPropertyWhiteList --global --actionName nextdescendents
```

read

Usage:

```
am> read SessionPropertyWhiteList --global
```

update

Usage:

```
am> update SessionPropertyWhiteList --global --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "defaults" : {
      "properties" : {
        "sessionPropertyWhitelist" : {
          "title" : "Whitelisted Session Property Names",
          "description" : "A list of properties that users may read, edit the value of, or delete from
 their session.<p><p> Adding properties to sessions can impact OpenAM's performance. Because there is
 no size constraint limiting the set of properties that you can add to sessions, and no limit on the
 number of session properties you can add, keep in mind that adding session properties can increase
 the load on an OpenAM deployment in the following areas: <ul><li>OpenAM server memory</li><li>OpenDJ
 storage</li><li>OpenDJ replication</li></ul><p>Protected attributes will NOT be allowed to be set,
 edited or deleted, even if they are included in this whitelist.",
```

```
          "propertyOrder" : 100,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "whitelistedQueryProperties" : {
          "title" : "Session Properties to return for session queries",
          "description" : "A list of session properties that can be returned to admins in a REST
 session query response.<p><p>This setting may impact REST query performance - when session properties
 are added, the CTS token must be retrieved, and will be the subject of decryption and decompression,
 if configured.<p><p> Protected attributes will NOT be allowed to be set, edited or deleted, even if
 they are included in this list.",
          "propertyOrder" : 110,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        }
      },
      "type" : "object",
      "title" : "Realm Defaults"
    }
  }
}
```

SessionUserService

Realm Operations

Resource path: `/users/{user}/services/session`

Resource version: `1.0`

create

Usage:

```
am> create SessionUserService --realm Realm --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "iplanet-am-session-quota-limit" : {
      "title" : "Active User Sessions",
      "description" : "Maximum number of concurrent CTS-based sessions OpenAM allows a user to have.",
      "propertyOrder" : 800,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "iplanet-am-session-max-caching-time" : {
      "title" : "Maximum Caching Time",
      "description" : "Maximum time that external clients of AM are recommended to cache the session
 for, in minutes.",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "iplanet-am-session-max-session-time" : {
      "title" : "Maximum Session Time",
      "description" : "Maximum time a session can remain valid before OpenAM requires the user to
 authenticate again, in minutes.",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "iplanet-am-session-max-idle-time" : {
      "title" : "Maximum Idle Time",
      "description" : "Maximum time a CTS-based session can remain idle before OpenAM requires the
 user to authenticate again, in minutes.",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    }
  }
}
```

delete

Usage:

```
am> delete SessionUserService --realm Realm
```

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action SessionUserService --realm Realm --user user --actionName getAllTypes
```

Parameters:

--user

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action SessionUserService --realm Realm --user user --actionName getCreatableTypes
```

Parameters:

--user

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action SessionUserService --realm Realm --user user --actionName nextdescendents
```

Parameters:

--user

read

Usage:

```
am> read SessionUserService --realm Realm
```

unassignServices

action.unassignServices.description

Usage:

```
am> action SessionUserService --realm Realm --body body --user user --actionName unassignServices
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "description" : "i18n:api-descriptor/UserServicesResource#schema.description",
  "type" : "object",
  "title" : "i18n:api-descriptor/UserServicesResource#schema.title",
  "properties" : {
    "serviceNames" : {
      "type" : "array",
      "title" : "i18n:api-descriptor/UserServicesResource#schema.servicename.title",
      "description" : "i18n:api-descriptor/UserServicesResource#schema.servicename.description",
      "items" : {
        "type" : "string"
      }
    }
  }
}
```

--user

update

Usage:

```
am> update SessionUserService --realm Realm --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "iplanet-am-session-quota-limit" : {
      "title" : "Active User Sessions",
      "description" : "Maximum number of concurrent CTS-based sessions OpenAM allows a user to have.",
      "propertyOrder" : 800,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "iplanet-am-session-max-caching-time" : {
      "title" : "Maximum Caching Time",
      "description" : "Maximum time that external clients of AM are recommended to cache the session
 for, in minutes.",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "integer",
```

```
      "exampleValue" : ""
    },
    "iplanet-am-session-max-session-time" : {
      "title" : "Maximum Session Time",
      "description" : "Maximum time a session can remain valid before OpenAM requires the user to
 authenticate again, in minutes.",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "iplanet-am-session-max-idle-time" : {
      "title" : "Maximum Idle Time",
      "description" : "Maximum time a CTS-based session can remain idle before OpenAM requires the
 user to authenticate again, in minutes.",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    }
  }
}
```

Sessions

Realm Operations

Represents Sessions that can queried via a REST interface.

Resource path: `/sessions`

Resource version: `4.0`

getSessionInfo

It reads and returns the information about the requested session.

Usage:

```
am> action Sessions --realm Realm --body body --actionName getSessionInfo
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "$schema" : "http://json-schema.org/draft-04/schema#",
  "description" : "Action request",
  "title" : "Action request",
  "type" : "object",
  "properties" : {
    "tokenId" : {
      "title" : "The tokenId",
      "description" : "The tokenId of the user you requests information for",
      "type" : "string"
    }
  },
  "required" : [ "tokenId" ]
}
```

getSessionInfoAndResetIdleTime

It reads and returns the information about the requested session. It also resets the session idle time.

Usage:

```
am> action Sessions --realm Realm --body body --actionName getSessionInfoAndResetIdleTime
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "$schema" : "http://json-schema.org/draft-04/schema#",
  "description" : "Action request",
  "title" : "Action request",
  "type" : "object",
  "properties" : {
    "tokenId" : {
      "title" : "The tokenId",
      "description" : "The tokenId of the user you requests information for",
      "type" : "string"
    }
  },
  "required" : [ "tokenId" ]
}
```

getSessionProperties

It reads and returns all of the whitelisted properties for the requested session.

Usage:

```
am> action Sessions --realm Realm --body body --actionName getSessionProperties
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "$schema" : "http://json-schema.org/draft-04/schema#",
  "description" : "Action request",
  "title" : "Action request",
  "type" : "object",
  "properties" : {
    "tokenId" : {
      "title" : "The tokenId",
      "description" : "The tokenId of the user you requests information for",
      "type" : "string"
    }
  },
  "required" : [ "tokenId" ]
}
```

logout

It does logout from OpenAM

Usage:

```
am> action Sessions --realm Realm --body body --actionName logout
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "$schema" : "http://json-schema.org/draft-04/schema#",
  "description" : "Action request",
  "title" : "Action request",
  "type" : "object",
  "properties" : {
    "tokenId" : {
      "title" : "The tokenId",
      "description" : "The tokenId of the user you requests information for",
      "type" : "string"
    }
  },
  "required" : [ "tokenId" ]
}
```

logoutByHandle

It logs out sessions based on the provided session handles.

Usage:

```
am> action Sessions --realm Realm --body body --actionName logoutByHandle
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "$schema" : "http://json-schema.org/draft-04/schema#",
  "description" : "Logout By Handle request",
  "type" : "object",
  "title" : "Logout By Handle request",
  "properties" : {
    "sessionHandles" : {
      "title" : "Session handles",
      "description" : "The array of session handles that needs to be invalidated.",
      "type" : "array",
      "items" : {
        "type" : "string"
      }
    }
  },
  "required" : [ "sessionHandles" ]
}
```

query

It queries all sessions using the provided query filter.

Usage:

```
am> query Sessions --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all. Fields that can be queried: [username, realm]

refresh

Suggests to OpenAM that it should refresh this session (update it's latest access time and reset its idleTime to 0). This will only be obeyed if the time between the session's previous latest access time and now is greater than the value configured for the server's Latest Access Time Update Frequency setting, which defaults to 60 seconds.

Usage:

```
am> action Sessions --realm Realm --body body --actionName refresh
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "$schema" : "http://json-schema.org/draft-04/schema#",
  "description" : "Action request",
  "title" : "Action request",
  "type" : "object",
  "properties" : {
    "tokenId" : {
      "title" : "The tokenId",
      "description" : "The tokenId of the user you requests information for",
      "type" : "string"
    }
  },
  "required" : [ "tokenId" ]
}
```

updateSessionProperties

It updates and returns all of the whitelisted properties for the requested session.

Usage:

```
am> action Sessions --realm Realm --body body --actionName updateSessionProperties
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "$schema" : "http://json-schema.org/draft-04/schema#",
  "description" : "Action request",
  "title" : "Action request",
  "type" : "object",
  "properties" : {
    "tokenId" : {
      "title" : "The tokenId",
      "description" : "The tokenId of the user you requests information for",
      "type" : "string"
    }
  },
  "required" : [ "tokenId" ]
}
```

validate

It checks that the specified SSO Token Id is valid or not. If there is any problem getting or validating the token which causes an exception the json response will be false. In addition if the token is expired then the json response will be set to false. Otherwise it will be set to true.

Usage:

```
am> action Sessions --realm Realm --body body --actionName validate
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "$schema" : "http://json-schema.org/draft-04/schema#",
  "description" : "Action request",
  "title" : "Action request",
  "type" : "object",
  "properties" : {
    "tokenId" : {
      "title" : "The tokenId",
      "description" : "The tokenId of the user you requests information for",
      "type" : "string"
    }
  },
  "required" : [ "tokenId" ]
}
```

SetPersistentCookie

Realm Operations

Resource path: `/realm-config/authentication/authenticationtrees/nodes/SetPersistentCookieNode`

Resource version: `1.0`

create

Usage:

```
am> create SetPersistentCookie --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
```

```
  "type" : "object",
  "properties" : {
    "useSecureCookie" : {
      "title" : "Use Secure Cookie",
      "description" : "Sets the persistent cookie as \"Secure\".",
      "propertyOrder" : 300,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "hmacSigningKey" : {
      "title" : "HMAC Signing Key",
      "description" : "Base64-encoded 256-bit key to use for HMAC signing of the cookie.",
      "propertyOrder" : 500,
      "type" : "string",
      "format" : "password",
      "exampleValue" : ""
    },
    "useHttpOnlyCookie" : {
      "title" : "Use HTTP Only Cookie",
      "description" : "Sets the persistent cookie as \"HttpOnly\".",
      "propertyOrder" : 400,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "idleTimeout" : {
      "title" : "Idle Timeout",
      "description" : "The maximum idle time between requests before the cookie is invalidated, in
 hours.",
      "propertyOrder" : 100,
      "type" : "integer",
      "exampleValue" : ""
    },
    "maxLife" : {
      "title" : "Max Life",
      "description" : "The maximum length of time the persistent cookie is valid for, in hours.",
      "propertyOrder" : 200,
      "type" : "integer",
      "exampleValue" : ""
    },
    "persistentCookieName" : {
      "title" : "Persistent Cookie Name",
      "description" : "Sets the name of the persistent cookie.",
      "propertyOrder" : 600,
      "type" : "string",
      "exampleValue" : ""
    }
  },
  "required" : [ "maxLife", "useSecureCookie", "useHttpOnlyCookie", "idleTimeout", "hmacSigningKey",
 "persistentCookieName" ]
}
```

delete

Usage:

```
am> delete SetPersistentCookie --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action SetPersistentCookie --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action SetPersistentCookie --realm Realm --actionName getCreatableTypes
```

listOutcomes

List the available outcomes for the node type.

Usage:

```
am> action SetPersistentCookie --realm Realm --body body --actionName listOutcomes
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "title" : "Some configuration of the node. This does not need to be complete against the
 configuration schema."
}
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action SetPersistentCookie --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query SetPersistentCookie --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read SetPersistentCookie --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update SetPersistentCookie --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "useSecureCookie" : {
      "title" : "Use Secure Cookie",
      "description" : "Sets the persistent cookie as \"Secure\".",
```

```
      "propertyOrder" : 300,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "hmacSigningKey" : {
      "title" : "HMAC Signing Key",
      "description" : "Base64-encoded 256-bit key to use for HMAC signing of the cookie.",
      "propertyOrder" : 500,
      "type" : "string",
      "format" : "password",
      "exampleValue" : ""
    },
    "useHttpOnlyCookie" : {
      "title" : "Use HTTP Only Cookie",
      "description" : "Sets the persistent cookie as \"HttpOnly\".",
      "propertyOrder" : 400,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "idleTimeout" : {
      "title" : "Idle Timeout",
      "description" : "The maximum idle time between requests before the cookie is invalidated, in
 hours.",
      "propertyOrder" : 100,
      "type" : "integer",
      "exampleValue" : ""
    },
    "maxLife" : {
      "title" : "Max Life",
      "description" : "The maximum length of time the persistent cookie is valid for, in hours.",
      "propertyOrder" : 200,
      "type" : "integer",
      "exampleValue" : ""
    },
    "persistentCookieName" : {
      "title" : "Persistent Cookie Name",
      "description" : "Sets the name of the persistent cookie.",
      "propertyOrder" : 600,
      "type" : "string",
      "exampleValue" : ""
    }
  },
  "required" : [ "maxLife", "useSecureCookie", "useHttpOnlyCookie", "idleTimeout", "hmacSigningKey",
 "persistentCookieName" ]
}
```


SetSessionProperties

Realm Operations

Resource path: `/realm-config/authentication/authenticationtrees/nodes/SetSessionPropertiesNode`

Resource version: `1.0`

create

Usage:

```
am> create SetSessionProperties --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "properties" : {
      "title" : "Properties",
      "description" : "The properties to set on the user's session if/when it is created.",
      "propertyOrder" : 100,
      "patternProperties" : {
        ".*" : {
          "type" : "string"
        }
      },
      "type" : "object",
      "exampleValue" : ""
    }
  },
  "required" : [ "properties" ]
}
```

delete

Usage:

```
am> delete SetSessionProperties --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action SetSessionProperties --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action SetSessionProperties --realm Realm --actionName getCreatableTypes
```

listOutcomes

List the available outcomes for the node type.

Usage:

```
am> action SetSessionProperties --realm Realm --body body --actionName listOutcomes
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "title" : "Some configuration of the node. This does not need to be complete against the
 configuration schema."
}
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action SetSessionProperties --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query SetSessionProperties --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read SetSessionProperties --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update SetSessionProperties --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "properties" : {
      "title" : "Properties",
      "description" : "The properties to set on the user's session if/when it is created.",
      "propertyOrder" : 100,
      "patternProperties" : {
        ".*" : {
          "type" : "string"
        }
      },
      "type" : "object",
      "exampleValue" : ""
    }
  },
  "required" : [ "properties" ]
}
```

SharedAgents

Realm Operations

Agents handler that is responsible for managing agents

Resource path: `/realm-config/agents/SharedAgent`

Resource version: `1.0`

create

Usage:

```
am> create SharedAgents --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "userpassword" : {
      "title" : "Password",
      "description" : "",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "format" : "password",
      "exampleValue" : ""
    },
    "status" : {
      "title" : "Status",
      "description" : "Status of the agent configuration.",
      "propertyOrder" : 200,
      "type" : "object",
      "exampleValue" : "",
      "properties" : {
        "inherited" : {
          "type" : "boolean",
          "required" : true
        },
        "value" : {
          "type" : "string",
          "required" : true
```

```
        }
      }
    },
    "agentProfilesAllowedToRead" : {
      "title" : "Agent Profiles allowed to Read.",
      "description" : "",
      "propertyOrder" : 22600,
      "items" : {
        "type" : "string"
      },
      "type" : "object",
      "exampleValue" : "",
      "properties" : {
        "inherited" : {
          "type" : "boolean",
          "required" : true
        },
        "value" : {
          "type" : "array",
          "required" : true
        }
      }
    },
    "cdssoRootUrl" : {
      "title" : "Agent Root URL for CDSSO",
      "description" : "The agent root URL for CDSSO. The valid value is in the following format:
 <br>protocol://hostname:port/<br> The protocol represents the protocol used, such as http or https.
 The hostname represents the host name of the machine on which the agent resides. The port represents
 the port number on which the agent is installed. The slash following the port number is required.",
      "propertyOrder" : 22700,
      "items" : {
        "type" : "string"
      },
      "type" : "object",
      "exampleValue" : "",
      "properties" : {
        "inherited" : {
          "type" : "boolean",
          "required" : true
        },
        "value" : {
          "type" : "array",
          "required" : true
        }
      }
    }
  }
}
```

delete

Usage:

```
am> delete SharedAgents --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action SharedAgents --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action SharedAgents --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action SharedAgents --realm Realm --actionName nextdescendents
```

query

Querying the agents of a specific type

Usage:

```
am> query SharedAgents --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read SharedAgents --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update SharedAgents --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "userpassword" : {
      "title" : "Password",
      "description" : "",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "format" : "password",
      "exampleValue" : ""
    },
    "status" : {
      "title" : "Status",
      "description" : "Status of the agent configuration.",
      "propertyOrder" : 200,
      "type" : "object",
      "exampleValue" : "",
      "properties" : {
        "inherited" : {
          "type" : "boolean",
          "required" : true
        },
        "value" : {
          "type" : "string",
          "required" : true
        }
      }
    },
    "agentProfilesAllowedToRead" : {
      "title" : "Agent Profiles allowed to Read.",
      "description" : "",
```

```
      "propertyOrder" : 22600,
      "items" : {
        "type" : "string"
      },
      "type" : "object",
      "exampleValue" : "",
      "properties" : {
        "inherited" : {
          "type" : "boolean",
          "required" : true
        },
        "value" : {
          "type" : "array",
          "required" : true
        }
      }
    },
    "cdssoRootUrl" : {
      "title" : "Agent Root URL for CDSSO",
      "description" : "The agent root URL for CDSSO. The valid value is in the following format:
 <br>protocol://hostname:port/<br> The protocol represents the protocol used, such as http or https.
 The hostname represents the host name of the machine on which the agent resides. The port represents
 the port number on which the agent is installed. The slash following the port number is required.",
      "propertyOrder" : 22700,
      "items" : {
        "type" : "string"
      },
      "type" : "object",
      "exampleValue" : "",
      "properties" : {
        "inherited" : {
          "type" : "boolean",
          "required" : true
        },
        "value" : {
          "type" : "array",
          "required" : true
        }
      }
    }
  }
}
```

Sites

Global Operations

This version 1.0 sites service represents a Sites resource with CQ operations on the users collection and CRUDPA operations available for the site item. Items can have server version 1.0 subresources.

Resource path: `/global-config/sites`

Resource version: `1.0`

create

Create new site entry

Usage:

```
am> create Sites --global --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "$schema" : "http://json-schema.org/draft-04/schema#",
  "description" : "Site schema.",
  "type" : "object",
  "title" : "Site schema",
  "properties" : {
    "_id" : {
      "type" : "string",
      "title" : "Name",
      "description" : "Site name."
    },
    "id" : {
      "type" : "string",
      "title" : "Site id",
      "description" : "Site's unique identifier.",
      "javaName" : "siteId"
    },
    "url" : {
      "type" : "string",
      "title" : "Primary URL",
      "description" : "Site primary URL."
    },
    "secondaryURLs" : {
      "type" : "array",
      "title" : "Secondary URLs",
      "description" : "Secondary URLs for this site.",
      "items" : {
        "type" : "string"
      }
    },
    "servers" : {
      "type" : "array",
      "title" : "Assigned Servers",
      "description" : "Servers assigned to this site.",
      "items" : {
        "type" : "object",
        "properties" : {
          "id" : {
            "type" : "string",
```

```
            "title" : "Server id",
            "description" : "Server's unique identifier for the site."
          },
          "url" : {
            "type" : "string",
            "title" : "Server URL",
            "description" : "Server URL of the site"
          }
        }
      }
    }
  }
}
```

delete

Delete site entry

Usage:

```
am> delete Sites --global --id id
```

Parameters:

--id

The unique identifier for the resource.

query

Query the collection of site entries

Usage:

```
am> query Sites --global --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all. Fields that can be queried: [_id, url]

read

Read a site entry

Usage:

```
am> read Sites --global --id id
```

Parameters:

--id

The unique identifier for the resource.

schema

Sites schema action that returns the sites schema json

Usage:

```
am> action Sites --global --actionName schema
```

template

Sites template action that returns a template json object for site insert

Usage:

```
am> action Sites --global --actionName template
```

update

Update a site entry

Usage:

```
am> update Sites --global --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "$schema" : "http://json-schema.org/draft-04/schema#",
  "description" : "Site schema.",
  "type" : "object",
  "title" : "Site schema",
  "properties" : {
    "_id" : {
      "type" : "string",
      "title" : "Name",
      "description" : "Site name."
    },
    "id" : {
      "type" : "string",
      "title" : "Site id",
      "description" : "Site's unique identifier.",
```

```
      "javaName" : "siteId"
    },
    "url" : {
      "type" : "string",
      "title" : "Primary URL",
      "description" : "Site primary URL."
    },
    "secondaryURLs" : {
      "type" : "array",
      "title" : "Secondary URLs",
      "description" : "Secondary URLs for this site.",
      "items" : {
        "type" : "string"
      }
    },
    "servers" : {
      "type" : "array",
      "title" : "Assigned Servers",
      "description" : "Servers assigned to this site.",
      "items" : {
        "type" : "object",
        "properties" : {
          "id" : {
            "type" : "string",
            "title" : "Server id",
            "description" : "Server's unique identifier for the site."
          },
          "url" : {
            "type" : "string",
            "title" : "Server URL",
            "description" : "Server URL of the site"
          }
        }
      }
    }
  }
}
```

SoapSTSAgentGroups

Realm Operations

Agent Groups handler that is responsible for managing agent groups

Resource path: `/realm-config/agents/groups/SoapSTSAgent`

Resource version: `1.0`

create

Usage:

```
am> create SoapSTSAgentGroups --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "publishServicePollInterval" : {
      "title" : "Poll Interval",
      "description" : "Interval, in seconds, to poll the sts publish service for newly-published SOAP
 STS instances.",
      "propertyOrder" : 26300,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    }
  }
}
```

delete

Usage:

```
am> delete SoapSTSAgentGroups --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action SoapSTSAgentGroups --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action SoapSTSAgentGroups --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action SoapSTSAgentGroups --realm Realm --actionName nextdescendents
```

query

Querying the agent groups of a specific type

Usage:

```
am> query SoapSTSAgentGroups --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read SoapSTSAgentGroups --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update SoapSTSAgentGroups --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "publishServicePollInterval" : {
      "title" : "Poll Interval",
      "description" : "Interval, in seconds, to poll the sts publish service for newly-published SOAP
 STS instances.",
      "propertyOrder" : 26300,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    }
  }
}
```

SoapStsAgents

Realm Operations

Agents handler that is responsible for managing agents

Resource path: `/realm-config/agents/SoapSTSAgent`

Resource version: `1.0`

create

Usage:

```
am> create SoapStsAgents --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "publishServicePollInterval" : {
      "title" : "Poll Interval",
```

```
      "description" : "Interval, in seconds, to poll the sts publish service for newly-published SOAP
 STS instances.",
      "propertyOrder" : 26300,
      "type" : "object",
      "exampleValue" : "",
      "properties" : {
        "inherited" : {
          "type" : "boolean",
          "required" : true
        },
        "value" : {
          "type" : "integer",
          "required" : true
        }
      }
    },
    "agentgroup" : {
      "title" : "Group",
      "description" : "Add the agent to a group to allow inheritance of property values from the
 group. <br>Changing the group will update inherited property values. <br>Inherited property values
 are copied to the agent.",
      "propertyOrder" : 50,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
    },
    "userpassword" : {
      "title" : "Password",
      "description" : "",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "format" : "password",
      "exampleValue" : ""
    }
  }
}
```


delete

Usage:

```
am> delete SoapStsAgents --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action SoapStsAgents --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action SoapStsAgents --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action SoapStsAgents --realm Realm --actionName nextdescendents
```

query

Querying the agents of a specific type

Usage:

```
am> query SoapStsAgents --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read SoapStsAgents --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update SoapStsAgents --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "publishServicePollInterval" : {
      "title" : "Poll Interval",
      "description" : "Interval, in seconds, to poll the sts publish service for newly-published SOAP
 STS instances.",
      "propertyOrder" : 26300,
      "type" : "object",
      "exampleValue" : "",
      "properties" : {
        "inherited" : {
          "type" : "boolean",
          "required" : true
        },
        "value" : {
          "type" : "integer",
          "required" : true
        }
      }
    },
    "agentgroup" : {
      "title" : "Group",
      "description" : "Add the agent to a group to allow inheritance of property values from the
 group. <br>Changing the group will update inherited property values. <br>Inherited property values
 are copied to the agent.",
      "propertyOrder" : 50,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
    },
    "userpassword" : {
      "title" : "Password",
      "description" : "",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "format" : "password",
      "exampleValue" : ""
    }
  }
}
```

SocialAuthInstagramModule

Realm Operations

Resource path: `/realm-config/authentication/modules/authSocialInstagram`

Resource version: `1.0`

create

Usage:

```
am> create SocialAuthInstagramModule --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "core" : {
      "type" : "object",
      "title" : "Core",
      "propertyOrder" : 0,
      "properties" : {
        "logoutServiceUrl" : {
          "title" : "OAuth 2.0 Provider Logout Service",
          "description" : "The URL of the Identity Provider's
 logout service.<br><br>To enable IdP logout, you must also add
 <code>org.forgerock.openam.authentication.modules.oauth2.OAuth2PostAuthnPlugin</code> to the
 <em>Authentication Post Processing Classes</em> setting. Navigate to Authentication > Settings > Post
 Authentication Processing.",
          "propertyOrder" : 2150,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "clientId" : {
          "title" : "Client Id",
          "description" : "OAuth client_id parameter<br><br>For more information on the OAuth
 client_id parameter refer to the <a href=\"http://tools.ietf.org/html/rfc6749#section-2.3.1\" target=
\"_blank\">RFC 6749</a>, section 2.3.1",
          "propertyOrder" : 400,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
```

```
      },
      "subjectProperty" : {
        "title" : "Subject Property",
        "description" : "Property used to identify which attribute an auth server identifies a user
by.",
        "propertyOrder" : 1100,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
      },
      "logoutBehaviour" : {
        "title" : "Logout Options",
        "description" : "Specify logout behavior.<br><br>The following options are available
for logging out of the OAuth 2.0 Provider when the user logs out of AM:<br/><ul><li>prompt:
Ask the user whether to log out from the OAuth 2.0 Provider</li><li>logout: Log out from
the OAuth 2.0 Provider without asking the user</li><li>donotlogout: Do not log out the
user from the OAuth 2.0 Provider</li></ul><br/>To enable IdP logout, you must also add
<code>org.forgerock.openam.authentication.modules.oauth2.OAuth2PostAuthnPlugin</code> to the
<em>Authentication Post Processing Classes</em> setting. Navigate to Authentication > Settings > Post
Authentication Processing.",
        "propertyOrder" : 2155,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
      },
      "provider" : {
        "title" : "Social Provider",
        "description" : "Social Provider for which this module is being setup.",
        "propertyOrder" : 200,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
      },
      "scope" : {
        "title" : "Scope",
        "description" : "OAuth scope; list of user profile properties<br><br>According to the OAuth
2.0 Authorization Framework, scope is a space-separated list of user profile attributes that the
client application requires. The list depends on the permissions that the resource owner grants to
the client application.<br/><br/> Some authorization servers use non-standard separators for scopes.
For example, Facebook takes a comma-separated list.<br/><br/>",
        "propertyOrder" : 900,
        "required" : true,
        "items" : {
          "type" : "string"
        },
        "minItems" : 1,
        "type" : "array",
        "exampleValue" : ""
      },
      "authenticationLevel" : {
        "title" : "Authentication Level",
        "description" : "The authentication level associated with this module.<br><br>Each
authentication module has an authentication level that can be used to indicate the level of security
associated with the module; 0 is the lowest (and the default).",
        "propertyOrder" : 100,
        "required" : true,
        "type" : "integer",
        "exampleValue" : ""
      },
```

```
        "tokenEndpoint" : {
          "title" : "Access Token Endpoint URL",
          "description" : "OAuth access token endpoint URL<br><br>This is the URL endpoint for
 access token retrieval provided by the OAuth Identity Provider. Refer to the <a href=\"http://
tools.ietf.org/html/rfc6749#section-3.2\" target=\"_blank\">RFC 6749</a>, section 3.2",
          "propertyOrder" : 700,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "usesBasicAuth" : {
          "title" : "Use Basic Auth",
          "description" : "When enabled, the client will use basic auth for authenticating with  the
 social auth provider. Enabled by default.",
          "propertyOrder" : 1200,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "clientSecret" : {
          "title" : "Client Secret",
          "description" : "OAuth client_secret parameter<br><br>For more information on the OAuth
 client_secret parameter refer to the <a href=\"http://tools.ietf.org/html/rfc6749#section-2.3.1\"
 target=\"_blank\">RFC 6749</a>, section 2.3.1",
          "propertyOrder" : 500,
          "required" : true,
          "type" : "string",
          "format" : "password",
          "exampleValue" : ""
        },
        "ssoProxyUrl" : {
          "title" : "Proxy URL",
          "description" : "The URL to the OpenAM OAuth proxy JSP<br><br>This URL should only be
 changed from the default, if an external server is performing the GET to POST proxying. The default
 is <code>/openam/oauth2c/OAuthProxy.jsp</code>",
          "propertyOrder" : 1300,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "authorizeEndpoint" : {
          "title" : "Authentication Endpoint URL",
          "description" : "OAuth authentication endpoint URL<br><br>This is the URL endpoint for OAuth
 authentication provided by the OAuth Identity Provider",
          "propertyOrder" : 600,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "userInfoEndpoint" : {
          "title" : "User Profile Service URL",
          "description" : "User profile information URL<br><br>This URL endpoint provides user profile
 information and is provided by the OAuth Identity Provider<br/><br/><i>NB </i>This URL should return
 JSON objects in response",
          "propertyOrder" : 800,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
```

```
        "scopeDelimiter" : {
          "title" : "Scope Delimiter",
          "description" : "Delimiter used to separate scope values. Default value is space.",
          "propertyOrder" : 1000,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "accountProvisioning" : {
      "type" : "object",
      "title" : "Account Provisioning",
      "propertyOrder" : 1,
      "properties" : {
        "enableRegistrationService" : {
          "title" : "Use IDM as Registration Service",
          "description" : "Whether to use IDM as an external Registration Service to complete
 registration for new users.<br><br>IDM is called and passed these parameters:<br/><br/
><ul><li><code>clientToken</code>: Signed, encrypted JWT of the OAuth 2.0 authentication state.</
li><li><code>returnParams</code>: Encoded URL parameters, required to be returned to AM to resume
 authentication after registration in IDM is complete.</li></ul>",
          "propertyOrder" : 1350,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "attributeMapperConfiguration" : {
          "title" : "Attribute Mapper Configuration",
          "description" : "Mapping of OAuth attributes to local OpenAM attributes<br><br>Attribute
 configuration that will be used to map the user info obtained from the OAuth 2.0 Provider to the
 local user data store in the OpenAM.<br/><br/>Example: <code>OAuth2.0_attribute=local_attribute</
code>",
          "propertyOrder" : 1800,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "accountProviderClass" : {
          "title" : "Account Provider",
          "description" : "Name of the class implementing the account provider.<br><br>This
 class is used by the module to find the account from the attributes mapped by the Account
 Mapper <code>org.forgerock.openam.authentication.modules.common.mapping.AccountProvider</code>
 interface.<br/>String constructor parameters can be provided by appending <code>|</code> separated
 values.",
          "propertyOrder" : 1400,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "anonymousUserName" : {
          "title" : "Anonymous User",
          "description" : "Username of the OpenAM anonymous user<br><br>The username of the user that
 will represent the anonymous user. This user account must already exist in the realm.",
          "propertyOrder" : 2100,
          "required" : true,
```

```
          "type" : "string",
          "exampleValue" : ""
        },
        "attributeMappingClasses" : {
          "title" : "Attribute Mapper",
          "description" : "Name of the class that implements the attribute
 mapping<br><br>This class maps the OAuth properties into OpenAM properties. A custom
 attribute mapper can be provided.<br/><br/>A custom attribute mapper must implement the
 <code>org.forgerock.openam.authentication.modules.common.mapping.AttributeMapper</code>
 interface.<br/>Provided implementations
 are:<ul><li>org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper</
li><li>org.forgerock.openam.authentication.modules.oidc.JwtAttributeMapper (can only be used when
 using the openid scope)</li></ul>String constructor parameters can be provided by appending <code>|</
code> separated values.",
          "propertyOrder" : 1700,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "mapToAnonymousUser" : {
          "title" : "Map to anonymous user",
          "description" : "Enabled anonymous user access to OpenAM for OAuth authenticated
 users<br><br>If selected, the authenticated users in the OAuth 2.0 Provider will be mapped to the
 anonymous user configured in the next parameter.<br/>If not selected the users authenticated will be
 mapped by the parameters configured in the account mapper.<br/><br/><i>NB </i>If <i>Create account if
 it does not exist</i> is enabled, that parameter takes precedence.",
          "propertyOrder" : 2000,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "saveAttributesInSession" : {
          "title" : "Save attributes in the session",
          "description" : "If this option is enabled, the attributes configured in the attribute
 mapper will be saved into the OpenAM session",
          "propertyOrder" : 2400,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "accountMapperConfiguration" : {
          "title" : "Account Mapper Configuration",
          "description" : "Mapping of OAuth account to local OpenAM account<br><br>Attribute
 configuration that will be used to map the account of the user authenticated in the OAuth 2.0
 Provider to the local data store in the OpenAM. Example: <code>OAuth2.0_attribute=local_attribute</
code>",
          "propertyOrder" : 1600,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "accountMapperClass" : {
          "title" : "Account Mapper",
```

```
          "description" : "Name of the class implementing the attribute mapping for the
 account search.<br><br>This class is used by the module to map from the account information
 received from the OAuth Identity Provider into OpenAM.<br/><br/>The class must implement
 the <code>org.forgerock.openam.authentication.modules.common.mapping.AttributeMapper</code>
 interface.<br/>Provided implementations
 are:<ul><li>org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper</
li><li>org.forgerock.openam.authentication.modules.oidc.JwtAttributeMapper (can only be used when
 using the openid scope)</li></ul>String constructor parameters can be provided by appending <code>|</
code> separated values.",
          "propertyOrder" : 1500,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "createAccount" : {
          "title" : "Create account if it does not exist",
          "description" : "If the OAuth2 account does not exist in the local OpenAM data store, an
 account will be created dynamically.<br><br>If this is enabled, the account mapper could create
 the account dynamically if there is no account mapped. Before creating the account, a dialog
 prompting for a password and asking for an activation code can be shown if the parameter \"Prompt
 for password setting and activation code\" is enabled.<br /><br />If this flag is not enabled, 3
 alternative options exist:<br/><br/><ol><li>The accounts need to have a user profile in the OpenAM
 User Data Store</li><li>The user does not have a user profile and the \"Ignore Profile\" is set in
 the Authentication Service of the realm.</li><li>The account is mapped to an anonymous account (see
 parameter \"Map to anonymous user\" and \"Anonymous User\")</li></ol>",
          "propertyOrder" : 1360,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        }
      }
    }
  }
}
```

delete

Usage:

```
am> delete SocialAuthInstagramModule --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action SocialAuthInstagramModule --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action SocialAuthInstagramModule --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action SocialAuthInstagramModule --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query SocialAuthInstagramModule --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read SocialAuthInstagramModule --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update SocialAuthInstagramModule --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "core" : {
      "type" : "object",
      "title" : "Core",
      "propertyOrder" : 0,
      "properties" : {
        "logoutServiceUrl" : {
          "title" : "OAuth 2.0 Provider Logout Service",
          "description" : "The URL of the Identity Provider's
 logout service.<br><br>To enable IdP logout, you must also add
 <code>org.forgerock.openam.authentication.modules.oauth2.OAuth2PostAuthnPlugin</code> to the
 <em>Authentication Post Processing Classes</em> setting. Navigate to Authentication > Settings > Post
 Authentication Processing.",
          "propertyOrder" : 2150,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "clientId" : {
          "title" : "Client Id",
          "description" : "OAuth client_id parameter<br><br>For more information on the OAuth
 client_id parameter refer to the <a href=\"http://tools.ietf.org/html/rfc6749#section-2.3.1\" target=
\"_blank\">RFC 6749</a>, section 2.3.1",
          "propertyOrder" : 400,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "subjectProperty" : {
          "title" : "Subject Property",
          "description" : "Property used to identify which attribute an auth server identifies a user
 by.",
          "propertyOrder" : 1100,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "logoutBehaviour" : {
          "title" : "Logout Options",
          "description" : "Specify logout behavior.<br><br>The following options are available
 for logging out of the OAuth 2.0 Provider when the user logs out of AM:<br/><ul><li>prompt:
 Ask the user whether to log out from the OAuth 2.0 Provider</li><li>logout: Log out from
 the OAuth 2.0 Provider without asking the user</li><li>donotlogout: Do not log out the
 user from the OAuth 2.0 Provider</li></ul><br/>To enable IdP logout, you must also add
 <code>org.forgerock.openam.authentication.modules.oauth2.OAuth2PostAuthnPlugin</code> to the
 <em>Authentication Post Processing Classes</em> setting. Navigate to Authentication > Settings > Post
 Authentication Processing.",
          "propertyOrder" : 2155,
          "required" : true,
```

```
          "type" : "string",
          "exampleValue" : ""
        },
        "provider" : {
          "title" : "Social Provider",
          "description" : "Social Provider for which this module is being setup.",
          "propertyOrder" : 200,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "scope" : {
          "title" : "Scope",
          "description" : "OAuth scope; list of user profile properties<br><br>According to the OAuth
 2.0 Authorization Framework, scope is a space-separated list of user profile attributes that the
 client application requires. The list depends on the permissions that the resource owner grants to
 the client application.<br/><br/> Some authorization servers use non-standard separators for scopes.
 For example, Facebook takes a comma-separated list.<br/><br/>",
          "propertyOrder" : 900,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "minItems" : 1,
          "type" : "array",
          "exampleValue" : ""
        },
        "authenticationLevel" : {
          "title" : "Authentication Level",
          "description" : "The authentication level associated with this module.<br><br>Each
 authentication module has an authentication level that can be used to indicate the level of security
 associated with the module; 0 is the lowest (and the default).",
          "propertyOrder" : 100,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "tokenEndpoint" : {
          "title" : "Access Token Endpoint URL",
          "description" : "OAuth access token endpoint URL<br><br>This is the URL endpoint for
 access token retrieval provided by the OAuth Identity Provider. Refer to the <a href=\"http://
tools.ietf.org/html/rfc6749#section-3.2\" target=\"_blank\">RFC 6749</a>, section 3.2",
          "propertyOrder" : 700,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "usesBasicAuth" : {
          "title" : "Use Basic Auth",
          "description" : "When enabled, the client will use basic auth for authenticating with  the
 social auth provider. Enabled by default.",
          "propertyOrder" : 1200,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "clientSecret" : {
          "title" : "Client Secret",
```

```
          "description" : "OAuth client_secret parameter<br><br>For more information on the OAuth
 client_secret parameter refer to the <a href=\"http://tools.ietf.org/html/rfc6749#section-2.3.1\"
 target=\"_blank\">RFC 6749</a>, section 2.3.1",
          "propertyOrder" : 500,
          "required" : true,
          "type" : "string",
          "format" : "password",
          "exampleValue" : ""
        },
        "ssoProxyUrl" : {
          "title" : "Proxy URL",
          "description" : "The URL to the OpenAM OAuth proxy JSP<br><br>This URL should only be
 changed from the default, if an external server is performing the GET to POST proxying. The default
 is <code>/openam/oauth2c/OAuthProxy.jsp</code>",
          "propertyOrder" : 1300,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "authorizeEndpoint" : {
          "title" : "Authentication Endpoint URL",
          "description" : "OAuth authentication endpoint URL<br><br>This is the URL endpoint for OAuth
 authentication provided by the OAuth Identity Provider",
          "propertyOrder" : 600,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "userInfoEndpoint" : {
          "title" : "User Profile Service URL",
          "description" : "User profile information URL<br><br>This URL endpoint provides user profile
 information and is provided by the OAuth Identity Provider<br/><br/><i>NB </i>This URL should return
 JSON objects in response",
          "propertyOrder" : 800,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "scopeDelimiter" : {
          "title" : "Scope Delimiter",
          "description" : "Delimiter used to separate scope values. Default value is space.",
          "propertyOrder" : 1000,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "accountProvisioning" : {
      "type" : "object",
      "title" : "Account Provisioning",
      "propertyOrder" : 1,
      "properties" : {
        "enableRegistrationService" : {
          "title" : "Use IDM as Registration Service",
          "description" : "Whether to use IDM as an external Registration Service to complete
 registration for new users.<br><br>IDM is called and passed these parameters:<br/><br/
></ul><li><code>clientToken</code>: Signed, encrypted JWT of the OAuth 2.0 authentication state.</
```

```
li><li><code>returnParams</code>: Encoded URL parameters, required to be returned to AM to resume
 authentication after registration in IDM is complete.</li></ul>",
          "propertyOrder" : 1350,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "attributeMapperConfiguration" : {
          "title" : "Attribute Mapper Configuration",
          "description" : "Mapping of OAuth attributes to local OpenAM attributes<br><br>Attribute
 configuration that will be used to map the user info obtained from the OAuth 2.0 Provider to the
 local user data store in the OpenAM.<br/><br/>Example: <code>OAuth2.0_attribute=local_attribute</
code>",
          "propertyOrder" : 1800,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "accountProviderClass" : {
          "title" : "Account Provider",
          "description" : "Name of the class implementing the account provider.<br><br>This
 class is used by the module to find the account from the attributes mapped by the Account
 Mapper <code>org.forgerock.openam.authentication.modules.common.mapping.AccountProvider</code>
 interface.<br/>String constructor parameters can be provided by appending <code>|</code> separated
 values.",
          "propertyOrder" : 1400,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "anonymousUserName" : {
          "title" : "Anonymous User",
          "description" : "Username of the OpenAM anonymous user<br><br>The username of the user that
 will represent the anonymous user. This user account must already exist in the realm.",
          "propertyOrder" : 2100,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "attributeMappingClasses" : {
          "title" : "Attribute Mapper",
          "description" : "Name of the class that implements the attribute
 mapping<br><br>This class maps the OAuth properties into OpenAM properties. A custom
 attribute mapper can be provided.<br/><br/>A custom attribute mapper must implement the
 <code>org.forgerock.openam.authentication.modules.common.mapping.AttributeMapper</code>
 interface.<br/>Provided implementations
 are:<ul><li>org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper</
li><li>org.forgerock.openam.authentication.modules.oidc.JwtAttributeMapper (can only be used when
 using the openid scope)</li></ul>String constructor parameters can be provided by appending <code>|</
code> separated values.",
          "propertyOrder" : 1700,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
```

```
          "exampleValue" : ""
        },
        "mapToAnonymousUser" : {
          "title" : "Map to anonymous user",
          "description" : "Enabled anonymous user access to OpenAM for OAuth authenticated
 users<br><br>If selected, the authenticated users in the OAuth 2.0 Provider will be mapped to the
 anonymous user configured in the next parameter.<br/>If not selected the users authenticated will be
 mapped by the parameters configured in the account mapper.<br/><br/><i>NB </i>If <i>Create account if
 it does not exist</i> is enabled, that parameter takes precedence.",
          "propertyOrder" : 2000,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "saveAttributesInSession" : {
          "title" : "Save attributes in the session",
          "description" : "If this option is enabled, the attributes configured in the attribute
 mapper will be saved into the OpenAM session",
          "propertyOrder" : 2400,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "accountMapperConfiguration" : {
          "title" : "Account Mapper Configuration",
          "description" : "Mapping of OAuth account to local OpenAM account<br><br>Attribute
 configuration that will be used to map the account of the user authenticated in the OAuth 2.0
 Provider to the local data store in the OpenAM. Example: <code>OAuth2.0_attribute=local_attribute</
code>",
          "propertyOrder" : 1600,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "accountMapperClass" : {
          "title" : "Account Mapper",
          "description" : "Name of the class implementing the attribute mapping for the
 account search.<br><br>This class is used by the module to map from the account information
 received from the OAuth Identity Provider into OpenAM.<br/><br/>The class must implement
 the <code>org.forgerock.openam.authentication.modules.common.mapping.AttributeMapper</code>
 interface.<br/>Provided implementations
 are:<ul><li>org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper</
li><li>org.forgerock.openam.authentication.modules.oidc.JwtAttributeMapper (can only be used when
 using the openid scope)</li></ul>String constructor parameters can be provided by appending <code>|</
code> separated values.",
          "propertyOrder" : 1500,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "createAccount" : {
          "title" : "Create account if it does not exist",
          "description" : "If the OAuth2 account does not exist in the local OpenAM data store, an
 account will be created dynamically.<br><br>If this is enabled, the account mapper could create
 the account dynamically if there is no account mapped. Before creating the account, a dialog
 prompting for a password and asking for an activation code can be shown if the parameter \"Prompt
```

```
 for password setting and activation code\" is enabled.<br /><br />If this flag is not enabled, 3
 alternative options exist:<br/><br/><ol><li>The accounts need to have a user profile in the OpenAM
 User Data Store</li><li>The user does not have a user profile and the \"Ignore Profile\" is set in
 the Authentication Service of the realm.</li><li>The account is mapped to an anonymous account (see
 parameter \"Map to anonymous user\" and \"Anonymous User\")</li></ol>",
          "propertyOrder" : 1360,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        }
      }
    }
  }
}
```

Global Operations

Resource path: `/global-config/authentication/modules/authSocialInstagram`

Resource version: `1.0`

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action SocialAuthInstagramModule --global --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action SocialAuthInstagramModule --global --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action SocialAuthInstagramModule --global --actionName nextdescendents
```

read

Usage:

```
am> read SocialAuthInstagramModule --global
```

update

Usage:

```
am> update SocialAuthInstagramModule --global --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "defaults" : {
      "properties" : {
        "core" : {
          "type" : "object",
          "title" : "Core",
          "propertyOrder" : 0,
          "properties" : {
            "userInfoEndpoint" : {
              "title" : "User Profile Service URL",
              "description" : "User profile information URL<br><br>This URL endpoint provides user
 profile information and is provided by the OAuth Identity Provider<br/><br/><i>NB </i>This URL should
 return JSON objects in response",
              "propertyOrder" : 800,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            },
            "scope" : {
              "title" : "Scope",
              "description" : "OAuth scope; list of user profile properties<br><br>According to the
 OAuth 2.0 Authorization Framework, scope is a space-separated list of user profile attributes that
 the client application requires. The list depends on the permissions that the resource owner grants
 to the client application.<br/><br/> Some authorization servers use non-standard separators for
 scopes. For example, Facebook takes a comma-separated list.<br/><br/>",
              "propertyOrder" : 900,
              "required" : true,
              "items" : {
                "type" : "string"
              },
              "type" : "array",
              "exampleValue" : ""
            },
            "clientSecret" : {
              "title" : "Client Secret",
              "description" : "OAuth client_secret parameter<br><br>For more information on the OAuth
 client_secret parameter refer to the <a href=\"http://tools.ietf.org/html/rfc6749#section-2.3.1\"
 target=\"_blank\">RFC 6749</a>, section 2.3.1",
              "propertyOrder" : 500,
              "required" : true,
```

```
              "type" : "string",
              "format" : "password",
              "exampleValue" : ""
            },
            "tokenEndpoint" : {
              "title" : "Access Token Endpoint URL",
              "description" : "OAuth access token endpoint URL<br><br>This is the URL endpoint for
 access token retrieval provided by the OAuth Identity Provider. Refer to the <a href=\"http://
tools.ietf.org/html/rfc6749#section-3.2\" target=\"_blank\">RFC 6749</a>, section 3.2",
              "propertyOrder" : 700,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            },
            "clientId" : {
              "title" : "Client Id",
              "description" : "OAuth client_id parameter<br><br>For more information on the OAuth
 client_id parameter refer to the <a href=\"http://tools.ietf.org/html/rfc6749#section-2.3.1\" target=
\"_blank\">RFC 6749</a>, section 2.3.1",
              "propertyOrder" : 400,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            },
            "logoutServiceUrl" : {
              "title" : "OAuth 2.0 Provider Logout Service",
              "description" : "The URL of the Identity Provider's
 logout service.<br><br>To enable IdP logout, you must also add
 <code>org.forgerock.openam.authentication.modules.oauth2.OAuth2PostAuthnPlugin</code> to the
 <em>Authentication Post Processing Classes</em> setting. Navigate to Authentication > Settings > Post
 Authentication Processing.",
              "propertyOrder" : 2150,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            },
            "subjectProperty" : {
              "title" : "Subject Property",
              "description" : "Property used to identify which attribute an auth server identifies a
 user by.",
              "propertyOrder" : 1100,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            },
            "authenticationLevel" : {
              "title" : "Authentication Level",
              "description" : "The authentication level associated with this module.<br><br>Each
 authentication module has an authentication level that can be used to indicate the level of security
 associated with the module; 0 is the lowest (and the default).",
              "propertyOrder" : 100,
              "required" : true,
              "type" : "integer",
              "exampleValue" : ""
            },
            "ssoProxyUrl" : {
              "title" : "Proxy URL",
```

```
              "description" : "The URL to the OpenAM OAuth proxy JSP<br><br>This URL should only be
 changed from the default, if an external server is performing the GET to POST proxying. The default
 is <code>/openam/oauth2c/OAuthProxy.jsp</code>",
              "propertyOrder" : 1300,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            },
            "usesBasicAuth" : {
              "title" : "Use Basic Auth",
              "description" : "When enabled, the client will use basic auth for authenticating with
 the social auth provider. Enabled by default.",
              "propertyOrder" : 1200,
              "required" : true,
              "type" : "boolean",
              "exampleValue" : ""
            },
            "scopeDelimiter" : {
              "title" : "Scope Delimiter",
              "description" : "Delimiter used to separate scope values. Default value is space.",
              "propertyOrder" : 1000,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            },
            "provider" : {
              "title" : "Social Provider",
              "description" : "Social Provider for which this module is being setup.",
              "propertyOrder" : 200,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            },
            "authorizeEndpoint" : {
              "title" : "Authentication Endpoint URL",
              "description" : "OAuth authentication endpoint URL<br><br>This is the URL endpoint for
 OAuth authentication provided by the OAuth Identity Provider",
              "propertyOrder" : 600,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            },
            "logoutBehaviour" : {
              "title" : "Logout Options",
              "description" : "Specify logout behavior.<br><br>The following options are
 available for logging out of the OAuth 2.0 Provider when the user logs out of AM:<br/
><ul><li>prompt: Ask the user whether to log out from the OAuth 2.0 Provider</li><li>logout:
 Log out from the OAuth 2.0 Provider without asking the user</li><li>donotlogout: Do not log
 out the user from the OAuth 2.0 Provider</li></ul><br/>To enable IdP logout, you must also add
 <code>org.forgerock.openam.authentication.modules.oauth2.OAuth2PostAuthnPlugin</code> to the
 <em>Authentication Post Processing Classes</em> setting. Navigate to Authentication > Settings > Post
 Authentication Processing.",
              "propertyOrder" : 2155,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            }
          }
        },
```

```
        "accountProvisioning" : {
          "type" : "object",
          "title" : "Account Provisioning",
          "propertyOrder" : 1,
          "properties" : {
            "accountProviderClass" : {
              "title" : "Account Provider",
              "description" : "Name of the class implementing the account provider.<br><br>This
 class is used by the module to find the account from the attributes mapped by the Account
 Mapper <code>org.forgerock.openam.authentication.modules.common.mapping.AccountProvider</code>
 interface.<br/>String constructor parameters can be provided by appending <code>|</code> separated
 values.",
              "propertyOrder" : 1400,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            },
            "attributeMapperConfiguration" : {
              "title" : "Attribute Mapper Configuration",
              "description" : "Mapping of OAuth attributes to local OpenAM attributes<br><br>Attribute
 configuration that will be used to map the user info obtained from the OAuth 2.0 Provider to the
 local user data store in the OpenAM.<br/><br/>Example: <code>OAuth2.0_attribute=local_attribute</
code>",
              "propertyOrder" : 1800,
              "required" : true,
              "items" : {
                "type" : "string"
              },
              "type" : "array",
              "exampleValue" : ""
            },
            "accountMapperConfiguration" : {
              "title" : "Account Mapper Configuration",
              "description" : "Mapping of OAuth account to local OpenAM account<br><br>Attribute
 configuration that will be used to map the account of the user authenticated in the OAuth 2.0
 Provider to the local data store in the OpenAM. Example: <code>OAuth2.0_attribute=local_attribute</
code>",
              "propertyOrder" : 1600,
              "required" : true,
              "items" : {
                "type" : "string"
              },
              "type" : "array",
              "exampleValue" : ""
            },
            "createAccount" : {
              "title" : "Create account if it does not exist",
              "description" : "If the OAuth2 account does not exist in the local OpenAM data store,
 an account will be created dynamically.<br><br>If this is enabled, the account mapper could create
 the account dynamically if there is no account mapped. Before creating the account, a dialog
 prompting for a password and asking for an activation code can be shown if the parameter \"Prompt
 for password setting and activation code\" is enabled.<br /><br />If this flag is not enabled, 3
 alternative options exist:<br/><br/><ol><li>The accounts need to have a user profile in the OpenAM
 User Data Store</li><li>The user does not have a user profile and the \"Ignore Profile\" is set in
 the Authentication Service of the realm.</li><li>The account is mapped to an anonymous account (see
 parameter \"Map to anonymous user\" and \"Anonymous User\")</li></ol>",
              "propertyOrder" : 1360,
              "required" : true,
              "type" : "boolean",
```

```
              "exampleValue" : ""
            },
            "enableRegistrationService" : {
              "title" : "Use IDM as Registration Service",
              "description" : "Whether to use IDM as an external Registration Service to
 complete registration for new users.<br><br>IDM is called and passed these parameters:<br/><br/
><ul><li><code>clientToken</code>: Signed, encrypted JWT of the OAuth 2.0 authentication state.</
li><li><code>returnParams</code>: Encoded URL parameters, required to be returned to AM to resume
 authentication after registration in IDM is complete.</li></ul>",
              "propertyOrder" : 1350,
              "required" : true,
              "type" : "boolean",
              "exampleValue" : ""
            },
            "accountMapperClass" : {
              "title" : "Account Mapper",
              "description" : "Name of the class implementing the attribute mapping for the
 account search.<br><br>This class is used by the module to map from the account information
 received from the OAuth Identity Provider into OpenAM.<br/><br/>The class must implement
 the <code>org.forgerock.openam.authentication.modules.common.mapping.AttributeMapper</code>
 interface.<br/>Provided implementations
 are:<ul><li>org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper</
li><li>org.forgerock.openam.authentication.modules.oidc.JwtAttributeMapper (can only be used when
 using the openid scope)</li></ul>String constructor parameters can be provided by appending <code>|</
code> separated values.",
              "propertyOrder" : 1500,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            },
            "attributeMappingClasses" : {
              "title" : "Attribute Mapper",
              "description" : "Name of the class that implements the attribute
 mapping<br><br>This class maps the OAuth properties into OpenAM properties. A custom
 attribute mapper can be provided.<br/><br/>A custom attribute mapper must implement the
 <code>org.forgerock.openam.authentication.modules.common.mapping.AttributeMapper</code>
 interface.<br/>Provided implementations
 are:<ul><li>org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper</
li><li>org.forgerock.openam.authentication.modules.oidc.JwtAttributeMapper (can only be used when
 using the openid scope)</li></ul>String constructor parameters can be provided by appending <code>|</
code> separated values.",
              "propertyOrder" : 1700,
              "required" : true,
              "items" : {
                "type" : "string"
              },
              "type" : "array",
              "exampleValue" : ""
            },
            "mapToAnonymousUser" : {
              "title" : "Map to anonymous user",
              "description" : "Enabled anonymous user access to OpenAM for OAuth authenticated
 users<br><br>If selected, the authenticated users in the OAuth 2.0 Provider will be mapped to the
 anonymous user configured in the next parameter.<br/>If not selected the users authenticated will be
 mapped by the parameters configured in the account mapper.<br/><br/><i>NB </i>If <i>Create account if
 it does not exist</i> is enabled, that parameter takes precedence.",
              "propertyOrder" : 2000,
              "required" : true,
              "type" : "boolean",
```

```
              "exampleValue" : ""
            },
            "saveAttributesInSession" : {
              "title" : "Save attributes in the session",
              "description" : "If this option is enabled, the attributes configured in the attribute
 mapper will be saved into the OpenAM session",
              "propertyOrder" : 2400,
              "required" : true,
              "type" : "boolean",
              "exampleValue" : ""
            },
            "anonymousUserName" : {
              "title" : "Anonymous User",
              "description" : "Username of the OpenAM anonymous user<br><br>The username of the user
 that will represent the anonymous user. This user account must already exist in the realm.",
              "propertyOrder" : 2100,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            }
          }
        }
      },
      "type" : "object",
      "title" : "Realm Defaults"
    }
  }
}
```

SocialAuthOAuth2Module

Realm Operations

Resource path: `/realm-config/authentication/modules/authSocialOAuth2`

Resource version: `1.0`

create

Usage:

```
am> create SocialAuthOAuth2Module --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "accountProvisioning" : {
      "type" : "object",
      "title" : "Account Provisioning",
      "propertyOrder" : 1,
      "properties" : {
        "enableRegistrationService" : {
          "title" : "Use IDM as Registration Service",
          "description" : "Whether to use IDM as an external Registration Service to complete
 registration for new users.<br><br>IDM is called and passed these parameters:<br/><br/
><ul><li><code>clientToken</code>: Signed, encrypted JWT of the OAuth 2.0 authentication state.</
li><li><code>returnParams</code>: Encoded URL parameters, required to be returned to AM to resume
 authentication after registration in IDM is complete.</li></ul>",
          "propertyOrder" : 1350,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "accountMapperConfiguration" : {
          "title" : "Account Mapper Configuration",
          "description" : "Mapping of OAuth account to local OpenAM account<br><br>Attribute
 configuration that will be used to map the account of the user authenticated in the OAuth 2.0
 Provider to the local data store in the OpenAM. Example: <code>OAuth2.0_attribute=local_attribute</
code>",
          "propertyOrder" : 1600,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : "sub=uid"
        },
        "accountMapperClass" : {
          "title" : "Account Mapper",
          "description" : "Name of the class implementing the attribute mapping for the
 account search.<br><br>This class is used by the module to map from the account information
 received from the OAuth Identity Provider into OpenAM.<br/><br/>The class must implement
 the <code>org.forgerock.openam.authentication.modules.common.mapping.AttributeMapper</code>
 interface.<br/>Provided implementations
 are:<ul><li>org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper</
li><li>org.forgerock.openam.authentication.modules.oidc.JwtAttributeMapper (can only be used when
 using the openid scope)</li></ul>String constructor parameters can be provided by appending <code>|</
code> separated values.",
          "propertyOrder" : 1500,
          "required" : true,
          "type" : "string",
          "exampleValue" :
 "org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper|*|google-"
        },
        "createAccount" : {
          "title" : "Create account if it does not exist",
          "description" : "If the OAuth2 account does not exist in the local OpenAM data store, an
 account will be created dynamically.<br><br>If this is enabled, the account mapper could create
```

```
 the account dynamically if there is no account mapped. Before creating the account, a dialog
 prompting for a password and asking for an activation code can be shown if the parameter \"Prompt
 for password setting and activation code\" is enabled.<br /><br />If this flag is not enabled, 3
 alternative options exist:<br/><br/><ol><li>The accounts need to have a user profile in the OpenAM
 User Data Store</li><li>The user does not have a user profile and the \"Ignore Profile\" is set in
 the Authentication Service of the realm.</li><li>The account is mapped to an anonymous account (see
 parameter \"Map to anonymous user\" and \"Anonymous User\")</li></ol>",
          "propertyOrder" : 1360,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "mapToAnonymousUser" : {
          "title" : "Map to anonymous user",
          "description" : "Enabled anonymous user access to OpenAM for OAuth authenticated
 users<br><br>If selected, the authenticated users in the OAuth 2.0 Provider will be mapped to the
 anonymous user configured in the next parameter.<br/>If not selected the users authenticated will be
 mapped by the parameters configured in the account mapper.<br/><br/><i>NB </i>If <i>Create account if
 it does not exist</i> is enabled, that parameter takes precedence.",
          "propertyOrder" : 2000,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "saveAttributesInSession" : {
          "title" : "Save attributes in the session",
          "description" : "If this option is enabled, the attributes configured in the attribute
 mapper will be saved into the OpenAM session",
          "propertyOrder" : 2400,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "promptPasswordFlag" : {
          "title" : "Prompt for password setting and activation code",
          "description" : "Users must set a password and complete the activation flow during dynamic
 profile creation.<br><br>If this is enabled, the user must set a password before the system creates
 an account dynamically and an activation code will be sent to the user's email address. The account
 will be created only if the password and activation code are properly set. <br />If this is disabled,
 the account will be created transparently without prompting the user.",
          "propertyOrder" : 1905,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "attributeMapperConfiguration" : {
          "title" : "Attribute Mapper Configuration",
          "description" : "Mapping of OAuth attributes to local OpenAM attributes<br><br>Attribute
 configuration that will be used to map the user info obtained from the OAuth 2.0 Provider to the
 local user data store in the OpenAM.<br/><br/>Example: <code>OAuth2.0_attribute=local_attribute</
code>",
          "propertyOrder" : 1800,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : "given_name=givenName family_name=sn name=cn email=mail sub=uid"
        },
```

```
        "attributeMappingClasses" : {
          "title" : "Attribute Mapper",
          "description" : "Name of the class that implements the attribute
 mapping<br><br>This class maps the OAuth properties into OpenAM properties. A custom
 attribute mapper can be provided.<br/><br/>A custom attribute mapper must implement the
 <code>org.forgerock.openam.authentication.modules.common.mapping.AttributeMapper</code>
 interface.<br/>Provided implementations
 are:<ul><li>org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper</
li><li>org.forgerock.openam.authentication.modules.oidc.JwtAttributeMapper (can only be used when
 using the openid scope)</li></ul>String constructor parameters can be provided by appending <code>|</
code> separated values.",
          "propertyOrder" : 1700,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" :
 "org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper|uid|google-"
        },
        "accountProviderClass" : {
          "title" : "Account Provider",
          "description" : "Name of the class implementing the account provider.<br><br>This
 class is used by the module to find the account from the attributes mapped by the Account
 Mapper <code>org.forgerock.openam.authentication.modules.common.mapping.AccountProvider</code>
 interface.<br/>String constructor parameters can be provided by appending <code>|</code> separated
 values.",
          "propertyOrder" : 1400,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "anonymousUserName" : {
          "title" : "Anonymous User",
          "description" : "Username of the OpenAM anonymous user<br><br>The username of the user that
 will represent the anonymous user. This user account must already exist in the realm.",
          "propertyOrder" : 2100,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "core" : {
      "type" : "object",
      "title" : "Core",
      "propertyOrder" : 0,
      "properties" : {
        "logoutServiceUrl" : {
          "title" : "OAuth 2.0 Provider Logout Service",
          "description" : "The URL of the Identity Provider's
 logout service.<br><br>To enable IdP logout, you must also add
 <code>org.forgerock.openam.authentication.modules.oauth2.OAuth2PostAuthnPlugin</code> to the
 <em>Authentication Post Processing Classes</em> setting. Navigate to Authentication > Settings > Post
 Authentication Processing.",
          "propertyOrder" : 2150,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
```

```
        },
        "authenticationLevel" : {
          "title" : "Authentication Level",
          "description" : "The authentication level associated with this module.<br><br>Each
 authentication module has an authentication level that can be used to indicate the level of security
 associated with the module; 0 is the lowest (and the default).",
          "propertyOrder" : 100,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "tokenEndpoint" : {
          "title" : "Access Token Endpoint URL",
          "description" : "OAuth access token endpoint URL<br><br>This is the URL endpoint for
 access token retrieval provided by the OAuth Identity Provider. Refer to the <a href=\"http://
tools.ietf.org/html/rfc6749#section-3.2\" target=\"_blank\">RFC 6749</a>, section 3.2",
          "propertyOrder" : 700,
          "required" : true,
          "type" : "string",
          "exampleValue" : "https://www.googleapis.com/oauth2/v4/token"
        },
        "clientId" : {
          "title" : "Client Id",
          "description" : "OAuth client_id parameter<br><br>For more information on the OAuth
 client_id parameter refer to the <a href=\"http://tools.ietf.org/html/rfc6749#section-2.3.1\" target=
\"_blank\">RFC 6749</a>, section 2.3.1",
          "propertyOrder" : 400,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "authorizeEndpoint" : {
          "title" : "Authentication Endpoint URL",
          "description" : "OAuth authentication endpoint URL<br><br>This is the URL endpoint for OAuth
 authentication provided by the OAuth Identity Provider",
          "propertyOrder" : 600,
          "required" : true,
          "type" : "string",
          "exampleValue" : "https://accounts.google.com/o/oauth2/v2/auth"
        },
        "issuerName" : {
          "title" : "Token Issuer",
          "description" : "Required when the 'openid' scope is included. Value must match the iss
 field in issued ID Token<br/>e.g. accounts.google.com<br><br>The issuer value MUST be provided when
 OAuth 2.0 Mix-Up Mitigation is enabled.",
          "propertyOrder" : 2500,
          "required" : true,
          "type" : "string",
          "exampleValue" : "https://accounts.google.com"
        },
        "scope" : {
          "title" : "Scope",
          "description" : "OAuth scope; list of user profile properties<br><br>According to the OAuth
 2.0 Authorization Framework, scope is a space-separated list of user profile attributes that the
 client application requires. The list depends on the permissions that the resource owner grants to
 the client application.<br/><br/> Some authorization servers use non-standard separators for scopes.
 For example, Facebook takes a comma-separated list.<br/><br/>",
          "propertyOrder" : 900,
          "required" : true,
```

```
          "items" : {
            "type" : "string"
          },
          "minItems" : 1,
          "type" : "array",
          "exampleValue" : "profile email"
        },
        "provider" : {
          "title" : "Social Provider",
          "description" : "Social Provider for which this module is being setup.",
          "propertyOrder" : 200,
          "required" : true,
          "type" : "string",
          "exampleValue" : "Google"
        },
        "ssoProxyUrl" : {
          "title" : "Proxy URL",
          "description" : "The URL to the OpenAM OAuth proxy JSP<br><br>This URL should only be
changed from the default, if an external server is performing the GET to POST proxying. The default
is <code>/openam/oauth2c/OAuthProxy.jsp</code>",
          "propertyOrder" : 1300,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "logoutBehaviour" : {
          "title" : "Logout Options",
          "description" : "Specify logout behavior.<br><br>The following options are available
for logging out of the OAuth 2.0 Provider when the user logs out of AM:<br/><ul><li>prompt:
Ask the user whether to log out from the OAuth 2.0 Provider</li><li>logout: Log out from
the OAuth 2.0 Provider without asking the user</li><li>donotlogout: Do not log out the
user from the OAuth 2.0 Provider</li></ul><br/>To enable IdP logout, you must also add
<code>org.forgerock.openam.authentication.modules.oauth2.OAuth2PostAuthnPlugin</code> to the
<em>Authentication Post Processing Classes</em> setting. Navigate to Authentication > Settings > Post
Authentication Processing.",
          "propertyOrder" : 2155,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "scopeDelimiter" : {
          "title" : "Scope Delimiter",
          "description" : "Delimiter used to separate scope values. Default value is space.",
          "propertyOrder" : 1000,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "subjectProperty" : {
          "title" : "Subject Property",
          "description" : "Property used to identify which attribute an auth server identifies a user
by.",
          "propertyOrder" : 1100,
          "required" : true,
          "type" : "string",
          "exampleValue" : "sub"
        },
        "mixUpMitigation" : {
          "title" : "OAuth 2.0 Mix-Up Mitigation enabled",
```

```
          "description" : "Enables OAuth 2.0 mix-up mitigation<br><br>The authorization
 server must support the <a href=\"https://tools.ietf.org/html/draft-ietf-oauth-mix-up-
mitigation-01#section-3.1\">OAuth 2.0 Mix-Up Mitigation draft</a>, otherwise OpenAM will fail to
 validate responses from the authorization server. If only the OAuth 2.0 protocol is utilized, make
 sure that the accepted issuer value is set in the \"Token Issuer\" setting.",
          "propertyOrder" : 2600,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "usesBasicAuth" : {
          "title" : "Use Basic Auth",
          "description" : "When enabled, the client will use basic auth for authenticating with  the
 social auth provider. Enabled by default.",
          "propertyOrder" : 1200,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "clientSecret" : {
          "title" : "Client Secret",
          "description" : "OAuth client_secret parameter<br><br>For more information on the OAuth
 client_secret parameter refer to the <a href=\"http://tools.ietf.org/html/rfc6749#section-2.3.1\"
 target=\"_blank\">RFC 6749</a>, section 2.3.1",
          "propertyOrder" : 500,
          "required" : true,
          "type" : "string",
          "format" : "password",
          "exampleValue" : ""
        },
        "userInfoEndpoint" : {
          "title" : "User Profile Service URL",
          "description" : "User profile information URL<br><br>This URL endpoint provides user profile
 information and is provided by the OAuth Identity Provider<br/><br/><i>NB </i>This URL should return
 JSON objects in response",
          "propertyOrder" : 800,
          "required" : true,
          "type" : "string",
          "exampleValue" : "https://www.googleapis.com/oauth2/v3/userinfo"
        }
      }
    },
    "emailSettings" : {
      "type" : "object",
      "title" : "Email",
      "propertyOrder" : 2,
      "properties" : {
        "smtpPassword" : {
          "title" : "SMTP User Password",
          "description" : "The Password of the SMTP User Name",
          "propertyOrder" : 1935,
          "required" : true,
          "type" : "string",
          "format" : "password",
          "exampleValue" : ""
        },
        "smtpHost" : {
          "title" : "SMTP host",
          "description" : "The mail host that will be used by the Email Gateway implementation",
```

```
          "propertyOrder" : 1920,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "smtpFromAddress" : {
          "title" : "SMTP From address",
          "description" : "The email address on behalf of whom the messages will be sent",
          "propertyOrder" : 1945,
          "required" : true,
          "type" : "string",
          "exampleValue" : "info@forgerock.com"
        },
        "smtpUsername" : {
          "title" : "SMTP User Name",
          "description" : "If the SMTP Service requires authentication, configure the user name here",
          "propertyOrder" : 1930,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "emailAttribute" : {
          "title" : "Email attribute in the Response",
          "description" : "Attribute from the response used to send activation code emails.<br><br>The
attribute in the response from the profile service of the Provider that contains the email address of
the authenticated user. This address will be used to send an email with an activation code when the
accounts are allowed to be created dynamically.",
          "propertyOrder" : 1910,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "emailGateway" : {
          "title" : "Mail Server Gateway implementation class",
          "description" : "The class used by the module to send email.<br><br>This class is used by
the module to send email. A custom implementation can be provided.<br/><br/>The custom implementation
must implement the <code>org.forgerock.openam.authentication.modules.oauth2.EmailGateway</code>",
          "propertyOrder" : 1915,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "smtpPort" : {
          "title" : "SMTP port",
          "description" : "The TCP port that will be used by the SMTP gateway",
          "propertyOrder" : 1925,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "smtpSslEnabled" : {
          "title" : "SMTP SSL Enabled",
          "description" : "Tick this option if the SMTP Server provides SSL",
          "propertyOrder" : 1940,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        }
      }
```

```
    }
  }
}
```

delete

Usage:

```
am> delete SocialAuthOAuth2Module --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action SocialAuthOAuth2Module --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action SocialAuthOAuth2Module --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action SocialAuthOAuth2Module --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query SocialAuthOAuth2Module --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read SocialAuthOAuth2Module --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update SocialAuthOAuth2Module --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "accountProvisioning" : {
      "type" : "object",
      "title" : "Account Provisioning",
      "propertyOrder" : 1,
      "properties" : {
        "enableRegistrationService" : {
          "title" : "Use IDM as Registration Service",
          "description" : "Whether to use IDM as an external Registration Service to complete
 registration for new users.<br><br>IDM is called and passed these parameters:<br/><br/
><ul><li><code>clientToken</code>: Signed, encrypted JWT of the OAuth 2.0 authentication state.</
li><li><code>returnParams</code>: Encoded URL parameters, required to be returned to AM to resume
 authentication after registration in IDM is complete.</li></ul>",
          "propertyOrder" : 1350,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "accountMapperConfiguration" : {
          "title" : "Account Mapper Configuration",
```

```
          "description" : "Mapping of OAuth account to local OpenAM account<br><br>Attribute
 configuration that will be used to map the account of the user authenticated in the OAuth 2.0
 Provider to the local data store in the OpenAM. Example: <code>OAuth2.0_attribute=local_attribute</
code>",
          "propertyOrder" : 1600,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : "sub=uid"
        },
        "accountMapperClass" : {
          "title" : "Account Mapper",
          "description" : "Name of the class implementing the attribute mapping for the
 account search.<br><br>This class is used by the module to map from the account information
 received from the OAuth Identity Provider into OpenAM.<br/><br/>The class must implement
 the <code>org.forgerock.openam.authentication.modules.common.mapping.AttributeMapper</code>
 interface.<br/>Provided implementations
 are:<ul><li>org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper</
li><li>org.forgerock.openam.authentication.modules.oidc.JwtAttributeMapper (can only be used when
 using the openid scope)</li></ul>String constructor parameters can be provided by appending <code>|</
code> separated values.",
          "propertyOrder" : 1500,
          "required" : true,
          "type" : "string",
          "exampleValue" :
 "org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper|*|google-"
        },
        "createAccount" : {
          "title" : "Create account if it does not exist",
          "description" : "If the OAuth2 account does not exist in the local OpenAM data store, an
 account will be created dynamically.<br><br>If this is enabled, the account mapper could create
 the account dynamically if there is no account mapped. Before creating the account, a dialog
 prompting for a password and asking for an activation code can be shown if the parameter \"Prompt
 for password setting and activation code\" is enabled.<br /><br />If this flag is not enabled, 3
 alternative options exist:<br/><br/><ol><li>The accounts need to have a user profile in the OpenAM
 User Data Store</li><li>The user does not have a user profile and the \"Ignore Profile\" is set in
 the Authentication Service of the realm.</li><li>The account is mapped to an anonymous account (see
 parameter \"Map to anonymous user\" and \"Anonymous User\")</li></ol>",
          "propertyOrder" : 1360,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "mapToAnonymousUser" : {
          "title" : "Map to anonymous user",
          "description" : "Enabled anonymous user access to OpenAM for OAuth authenticated
 users<br><br>If selected, the authenticated users in the OAuth 2.0 Provider will be mapped to the
 anonymous user configured in the next parameter.<br/>If not selected the users authenticated will be
 mapped by the parameters configured in the account mapper.<br/><br/><i>NB </i>If <i>Create account if
 it does not exist</i> is enabled, that parameter takes precedence.",
          "propertyOrder" : 2000,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "saveAttributesInSession" : {
          "title" : "Save attributes in the session",
```

```
          "description" : "If this option is enabled, the attributes configured in the attribute
 mapper will be saved into the OpenAM session",
          "propertyOrder" : 2400,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "promptPasswordFlag" : {
          "title" : "Prompt for password setting and activation code",
          "description" : "Users must set a password and complete the activation flow during dynamic
 profile creation.<br><br>If this is enabled, the user must set a password before the system creates
 an account dynamically and an activation code will be sent to the user's email address. The account
 will be created only if the password and activation code are properly set. <br />If this is disabled,
 the account will be created transparently without prompting the user.",
          "propertyOrder" : 1905,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "attributeMapperConfiguration" : {
          "title" : "Attribute Mapper Configuration",
          "description" : "Mapping of OAuth attributes to local OpenAM attributes<br><br>Attribute
 configuration that will be used to map the user info obtained from the OAuth 2.0 Provider to the
 local user data store in the OpenAM.<br/><br/>Example: <code>OAuth2.0_attribute=local_attribute</
code>",
          "propertyOrder" : 1800,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : "given_name=givenName family_name=sn name=cn email=mail sub=uid"
        },
        "attributeMappingClasses" : {
          "title" : "Attribute Mapper",
          "description" : "Name of the class that implements the attribute
 mapping<br><br>This class maps the OAuth properties into OpenAM properties. A custom
 attribute mapper can be provided.<br/><br/>A custom attribute mapper must implement the
 <code>org.forgerock.openam.authentication.modules.common.mapping.AttributeMapper</code>
 interface.<br/>Provided implementations
 are:<ul><li>org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper</
li><li>org.forgerock.openam.authentication.modules.oidc.JwtAttributeMapper (can only be used when
 using the openid scope)</li></ul>String constructor parameters can be provided by appending <code>|</
code> separated values.",
          "propertyOrder" : 1700,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" :
 "org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper|uid|google-"
        },
        "accountProviderClass" : {
          "title" : "Account Provider",
          "description" : "Name of the class implementing the account provider.<br><br>This
 class is used by the module to find the account from the attributes mapped by the Account
 Mapper <code>org.forgerock.openam.authentication.modules.common.mapping.AccountProvider</code>
```

```
 interface.<br/>String constructor parameters can be provided by appending <code>|</code> separated
 values.",
          "propertyOrder" : 1400,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "anonymousUserName" : {
          "title" : "Anonymous User",
          "description" : "Username of the OpenAM anonymous user<br><br>The username of the user that
 will represent the anonymous user. This user account must already exist in the realm.",
          "propertyOrder" : 2100,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "core" : {
      "type" : "object",
      "title" : "Core",
      "propertyOrder" : 0,
      "properties" : {
        "logoutServiceUrl" : {
          "title" : "OAuth 2.0 Provider Logout Service",
          "description" : "The URL of the Identity Provider's
 logout service.<br><br>To enable IdP logout, you must also add
 <code>org.forgerock.openam.authentication.modules.oauth2.OAuth2PostAuthnPlugin</code> to the
 <em>Authentication Post Processing Classes</em> setting. Navigate to Authentication > Settings > Post
 Authentication Processing.",
          "propertyOrder" : 2150,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "authenticationLevel" : {
          "title" : "Authentication Level",
          "description" : "The authentication level associated with this module.<br><br>Each
 authentication module has an authentication level that can be used to indicate the level of security
 associated with the module; 0 is the lowest (and the default).",
          "propertyOrder" : 100,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "tokenEndpoint" : {
          "title" : "Access Token Endpoint URL",
          "description" : "OAuth access token endpoint URL<br><br>This is the URL endpoint for
 access token retrieval provided by the OAuth Identity Provider. Refer to the <a href=\"http://
tools.ietf.org/html/rfc6749#section-3.2\" target=\"_blank\">RFC 6749</a>, section 3.2",
          "propertyOrder" : 700,
          "required" : true,
          "type" : "string",
          "exampleValue" : "https://www.googleapis.com/oauth2/v4/token"
        },
        "clientId" : {
          "title" : "Client Id",
```

```
          "description" : "OAuth client_id parameter<br><br>For more information on the OAuth
 client_id parameter refer to the <a href=\"http://tools.ietf.org/html/rfc6749#section-2.3.1\" target=
\"_blank\">RFC 6749</a>, section 2.3.1",
          "propertyOrder" : 400,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "authorizeEndpoint" : {
          "title" : "Authentication Endpoint URL",
          "description" : "OAuth authentication endpoint URL<br><br>This is the URL endpoint for OAuth
 authentication provided by the OAuth Identity Provider",
          "propertyOrder" : 600,
          "required" : true,
          "type" : "string",
          "exampleValue" : "https://accounts.google.com/o/oauth2/v2/auth"
        },
        "issuerName" : {
          "title" : "Token Issuer",
          "description" : "Required when the 'openid' scope is included. Value must match the iss
 field in issued ID Token<br/>e.g. accounts.google.com<br><br>The issuer value MUST be provided when
 OAuth 2.0 Mix-Up Mitigation is enabled.",
          "propertyOrder" : 2500,
          "required" : true,
          "type" : "string",
          "exampleValue" : "https://accounts.google.com"
        },
        "scope" : {
          "title" : "Scope",
          "description" : "OAuth scope; list of user profile properties<br><br>According to the OAuth
 2.0 Authorization Framework, scope is a space-separated list of user profile attributes that the
 client application requires. The list depends on the permissions that the resource owner grants to
 the client application.<br/><br/> Some authorization servers use non-standard separators for scopes.
 For example, Facebook takes a comma-separated list.<br/><br/>",
          "propertyOrder" : 900,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "minItems" : 1,
          "type" : "array",
          "exampleValue" : "profile email"
        },
        "provider" : {
          "title" : "Social Provider",
          "description" : "Social Provider for which this module is being setup.",
          "propertyOrder" : 200,
          "required" : true,
          "type" : "string",
          "exampleValue" : "Google"
        },
        "ssoProxyUrl" : {
          "title" : "Proxy URL",
          "description" : "The URL to the OpenAM OAuth proxy JSP<br><br>This URL should only be
 changed from the default, if an external server is performing the GET to POST proxying. The default
 is <code>/openam/oauth2c/OAuthProxy.jsp</code>",
          "propertyOrder" : 1300,
          "required" : true,
          "type" : "string",
```

```
          "exampleValue" : ""
        },
        "logoutBehaviour" : {
          "title" : "Logout Options",
          "description" : "Specify logout behavior.<br><br>The following options are available
 for logging out of the OAuth 2.0 Provider when the user logs out of AM:<br/><ul><li>prompt:
 Ask the user whether to log out from the OAuth 2.0 Provider</li><li>logout: Log out from
 the OAuth 2.0 Provider without asking the user</li><li>donotlogout: Do not log out the
 user from the OAuth 2.0 Provider</li></ul><br/>To enable IdP logout, you must also add
 <code>org.forgerock.openam.authentication.modules.oauth2.OAuth2PostAuthnPlugin</code> to the
 <em>Authentication Post Processing Classes</em> setting. Navigate to Authentication > Settings > Post
 Authentication Processing.",
          "propertyOrder" : 2155,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "scopeDelimiter" : {
          "title" : "Scope Delimiter",
          "description" : "Delimiter used to separate scope values. Default value is space.",
          "propertyOrder" : 1000,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "subjectProperty" : {
          "title" : "Subject Property",
          "description" : "Property used to identify which attribute an auth server identifies a user
 by.",
          "propertyOrder" : 1100,
          "required" : true,
          "type" : "string",
          "exampleValue" : "sub"
        },
        "mixUpMitigation" : {
          "title" : "OAuth 2.0 Mix-Up Mitigation enabled",
          "description" : "Enables OAuth 2.0 mix-up mitigation<br><br>The authorization
 server must support the <a href=\"https://tools.ietf.org/html/draft-ietf-oauth-mix-up-
mitigation-01#section-3.1\">OAuth 2.0 Mix-Up Mitigation draft</a>, otherwise OpenAM will fail to
 validate responses from the authorization server. If only the OAuth 2.0 protocol is utilized, make
 sure that the accepted issuer value is set in the \"Token Issuer\" setting.",
          "propertyOrder" : 2600,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "usesBasicAuth" : {
          "title" : "Use Basic Auth",
          "description" : "When enabled, the client will use basic auth for authenticating with  the
 social auth provider. Enabled by default.",
          "propertyOrder" : 1200,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "clientSecret" : {
          "title" : "Client Secret",
```

```
          "description" : "OAuth client_secret parameter<br><br>For more information on the OAuth
client_secret parameter refer to the <a href=\"http://tools.ietf.org/html/rfc6749#section-2.3.1\"
target=\"_blank\">RFC 6749</a>, section 2.3.1",
          "propertyOrder" : 500,
          "required" : true,
          "type" : "string",
          "format" : "password",
          "exampleValue" : ""
        },
        "userInfoEndpoint" : {
          "title" : "User Profile Service URL",
          "description" : "User profile information URL<br><br>This URL endpoint provides user profile
information and is provided by the OAuth Identity Provider<br/><br/><i>NB </i>This URL should return
JSON objects in response",
          "propertyOrder" : 800,
          "required" : true,
          "type" : "string",
          "exampleValue" : "https://www.googleapis.com/oauth2/v3/userinfo"
        }
      }
    },
    "emailSettings" : {
      "type" : "object",
      "title" : "Email",
      "propertyOrder" : 2,
      "properties" : {
        "smtpPassword" : {
          "title" : "SMTP User Password",
          "description" : "The Password of the SMTP User Name",
          "propertyOrder" : 1935,
          "required" : true,
          "type" : "string",
          "format" : "password",
          "exampleValue" : ""
        },
        "smtpHost" : {
          "title" : "SMTP host",
          "description" : "The mail host that will be used by the Email Gateway implementation",
          "propertyOrder" : 1920,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "smtpFromAddress" : {
          "title" : "SMTP From address",
          "description" : "The email address on behalf of whom the messages will be sent",
          "propertyOrder" : 1945,
          "required" : true,
          "type" : "string",
          "exampleValue" : "info@forgerock.com"
        },
        "smtpUsername" : {
          "title" : "SMTP User Name",
          "description" : "If the SMTP Service requires authentication, configure the user name here",
          "propertyOrder" : 1930,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
```

```
        "emailAttribute" : {
          "title" : "Email attribute in the Response",
          "description" : "Attribute from the response used to send activation code emails.<br><br>The
 attribute in the response from the profile service of the Provider that contains the email address of
 the authenticated user. This address will be used to send an email with an activation code when the
 accounts are allowed to be created dynamically.",
          "propertyOrder" : 1910,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "emailGateway" : {
          "title" : "Mail Server Gateway implementation class",
          "description" : "The class used by the module to send email.<br><br>This class is used by
 the module to send email. A custom implementation can be provided.<br/><br/>The custom implementation
 must implement the <code>org.forgerock.openam.authentication.modules.oauth2.EmailGateway</code>",
          "propertyOrder" : 1915,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "smtpPort" : {
          "title" : "SMTP port",
          "description" : "The TCP port that will be used by the SMTP gateway",
          "propertyOrder" : 1925,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "smtpSslEnabled" : {
          "title" : "SMTP SSL Enabled",
          "description" : "Tick this option if the SMTP Server provides SSL",
          "propertyOrder" : 1940,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        }
      }
    }
  }
}
```

Global Operations

Resource path: `/global-config/authentication/modules/authSocialOAuth2`

Resource version: `1.0`

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action SocialAuthOAuth2Module --global --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action SocialAuthOAuth2Module --global --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action SocialAuthOAuth2Module --global --actionName nextdescendents
```

read

Usage:

```
am> read SocialAuthOAuth2Module --global
```

update

Usage:

```
am> update SocialAuthOAuth2Module --global --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "defaults" : {
      "properties" : {
        "core" : {
          "type" : "object",
          "title" : "Core",
          "propertyOrder" : 0,
          "properties" : {
            "tokenEndpoint" : {
              "title" : "Access Token Endpoint URL",
              "description" : "OAuth access token endpoint URL<br><br>This is the URL endpoint for
 access token retrieval provided by the OAuth Identity Provider. Refer to the <a href=\"http://
tools.ietf.org/html/rfc6749#section-3.2\" target=\"_blank\">RFC 6749</a>, section 3.2",
```

```
              "propertyOrder" : 700,
              "required" : true,
              "type" : "string",
              "exampleValue" : "https://www.googleapis.com/oauth2/v4/token"
            },
            "clientId" : {
              "title" : "Client Id",
              "description" : "OAuth client_id parameter<br><br>For more information on the OAuth
 client_id parameter refer to the <a href=\"http://tools.ietf.org/html/rfc6749#section-2.3.1\" target=
\"_blank\">RFC 6749</a>, section 2.3.1",
              "propertyOrder" : 400,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            },
            "scope" : {
              "title" : "Scope",
              "description" : "OAuth scope; list of user profile properties<br><br>According to the
 OAuth 2.0 Authorization Framework, scope is a space-separated list of user profile attributes that
 the client application requires. The list depends on the permissions that the resource owner grants
 to the client application.<br/><br/> Some authorization servers use non-standard separators for
 scopes. For example, Facebook takes a comma-separated list.<br/><br/>",
              "propertyOrder" : 900,
              "required" : true,
              "items" : {
                "type" : "string"
              },
              "type" : "array",
              "exampleValue" : "profile email"
            },
            "ssoProxyUrl" : {
              "title" : "Proxy URL",
              "description" : "The URL to the OpenAM OAuth proxy JSP<br><br>This URL should only be
 changed from the default, if an external server is performing the GET to POST proxying. The default
 is <code>/openam/oauth2c/OAuthProxy.jsp</code>",
              "propertyOrder" : 1300,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            },
            "provider" : {
              "title" : "Social Provider",
              "description" : "Social Provider for which this module is being setup.",
              "propertyOrder" : 200,
              "required" : true,
              "type" : "string",
              "exampleValue" : "Google"
            },
            "clientSecret" : {
              "title" : "Client Secret",
              "description" : "OAuth client_secret parameter<br><br>For more information on the OAuth
 client_secret parameter refer to the <a href=\"http://tools.ietf.org/html/rfc6749#section-2.3.1\"
 target=\"_blank\">RFC 6749</a>, section 2.3.1",
              "propertyOrder" : 500,
              "required" : true,
              "type" : "string",
              "format" : "password",
              "exampleValue" : ""
            },
```

```
            "usesBasicAuth" : {
              "title" : "Use Basic Auth",
              "description" : "When enabled, the client will use basic auth for authenticating with
the social auth provider. Enabled by default.",
              "propertyOrder" : 1200,
              "required" : true,
              "type" : "boolean",
              "exampleValue" : ""
            },
            "userInfoEndpoint" : {
              "title" : "User Profile Service URL",
              "description" : "User profile information URL<br><br>This URL endpoint provides user
profile information and is provided by the OAuth Identity Provider<br/><br/><i>NB </i>This URL should
return JSON objects in response",
              "propertyOrder" : 800,
              "required" : true,
              "type" : "string",
              "exampleValue" : "https://www.googleapis.com/oauth2/v3/userinfo"
            },
            "issuerName" : {
              "title" : "Token Issuer",
              "description" : "Required when the 'openid' scope is included. Value must match the iss
field in issued ID Token<br/>e.g. accounts.google.com<br><br>The issuer value MUST be provided when
OAuth 2.0 Mix-Up Mitigation is enabled.",
              "propertyOrder" : 2500,
              "required" : true,
              "type" : "string",
              "exampleValue" : "https://accounts.google.com"
            },
            "subjectProperty" : {
              "title" : "Subject Property",
              "description" : "Property used to identify which attribute an auth server identifies a
user by.",
              "propertyOrder" : 1100,
              "required" : true,
              "type" : "string",
              "exampleValue" : "sub"
            },
            "logoutServiceUrl" : {
              "title" : "OAuth 2.0 Provider Logout Service",
              "description" : "The URL of the Identity Provider's
logout service.<br><br>To enable IdP logout, you must also add
<code>org.forgerock.openam.authentication.modules.oauth2.OAuth2PostAuthnPlugin</code> to the
<em>Authentication Post Processing Classes</em> setting. Navigate to Authentication > Settings > Post
Authentication Processing.",
              "propertyOrder" : 2150,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            },
            "authorizeEndpoint" : {
              "title" : "Authentication Endpoint URL",
              "description" : "OAuth authentication endpoint URL<br><br>This is the URL endpoint for
OAuth authentication provided by the OAuth Identity Provider",
              "propertyOrder" : 600,
              "required" : true,
              "type" : "string",
              "exampleValue" : "https://accounts.google.com/o/oauth2/v2/auth"
            },
```

```
            "authenticationLevel" : {
              "title" : "Authentication Level",
              "description" : "The authentication level associated with this module.<br><br>Each
 authentication module has an authentication level that can be used to indicate the level of security
 associated with the module; 0 is the lowest (and the default).",
              "propertyOrder" : 100,
              "required" : true,
              "type" : "integer",
              "exampleValue" : ""
            },
            "logoutBehaviour" : {
              "title" : "Logout Options",
              "description" : "Specify logout behavior.<br><br>The following options are
 available for logging out of the OAuth 2.0 Provider when the user logs out of AM:<br/
><ul><li>prompt: Ask the user whether to log out from the OAuth 2.0 Provider</li><li>logout:
 Log out from the OAuth 2.0 Provider without asking the user</li><li>donotlogout: Do not log
 out the user from the OAuth 2.0 Provider</li></ul><br/>To enable IdP logout, you must also add
 <code>org.forgerock.openam.authentication.modules.oauth2.OAuth2PostAuthnPlugin</code> to the
 <em>Authentication Post Processing Classes</em> setting. Navigate to Authentication > Settings > Post
 Authentication Processing.",
              "propertyOrder" : 2155,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            },
            "mixUpMitigation" : {
              "title" : "OAuth 2.0 Mix-Up Mitigation enabled",
              "description" : "Enables OAuth 2.0 mix-up mitigation<br><br>The authorization
 server must support the <a href=\"https://tools.ietf.org/html/draft-ietf-oauth-mix-up-
mitigation-01#section-3.1\">OAuth 2.0 Mix-Up Mitigation draft</a>, otherwise OpenAM will fail to
 validate responses from the authorization server. If only the OAuth 2.0 protocol is utilized, make
 sure that the accepted issuer value is set in the \"Token Issuer\" setting.",
              "propertyOrder" : 2600,
              "required" : true,
              "type" : "boolean",
              "exampleValue" : ""
            },
            "scopeDelimiter" : {
              "title" : "Scope Delimiter",
              "description" : "Delimiter used to separate scope values. Default value is space.",
              "propertyOrder" : 1000,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            }
          }
        },
        "accountProvisioning" : {
          "type" : "object",
          "title" : "Account Provisioning",
          "propertyOrder" : 1,
          "properties" : {
            "anonymousUserName" : {
              "title" : "Anonymous User",
              "description" : "Username of the OpenAM anonymous user<br><br>The username of the user
 that will represent the anonymous user. This user account must already exist in the realm.",
              "propertyOrder" : 2100,
              "required" : true,
              "type" : "string",
```

```
              "exampleValue" : ""
            },
            "saveAttributesInSession" : {
              "title" : "Save attributes in the session",
              "description" : "If this option is enabled, the attributes configured in the attribute
 mapper will be saved into the OpenAM session",
              "propertyOrder" : 2400,
              "required" : true,
              "type" : "boolean",
              "exampleValue" : ""
            },
            "accountMapperConfiguration" : {
              "title" : "Account Mapper Configuration",
              "description" : "Mapping of OAuth account to local OpenAM account<br><br>Attribute
 configuration that will be used to map the account of the user authenticated in the OAuth 2.0
 Provider to the local data store in the OpenAM. Example: <code>OAuth2.0_attribute=local_attribute</
code>",
              "propertyOrder" : 1600,
              "required" : true,
              "items" : {
                "type" : "string"
              },
              "type" : "array",
              "exampleValue" : "sub=uid"
            },
            "accountMapperClass" : {
              "title" : "Account Mapper",
              "description" : "Name of the class implementing the attribute mapping for the
 account search.<br><br>This class is used by the module to map from the account information
 received from the OAuth Identity Provider into OpenAM.<br/><br/>The class must implement
 the <code>org.forgerock.openam.authentication.modules.common.mapping.AttributeMapper</code>
 interface.<br/>Provided implementations
 are:<ul><li>org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper</
li><li>org.forgerock.openam.authentication.modules.oidc.JwtAttributeMapper (can only be used when
 using the openid scope)</li></ul>String constructor parameters can be provided by appending <code>|</
code> separated values.",
              "propertyOrder" : 1500,
              "required" : true,
              "type" : "string",
              "exampleValue" :
 "org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper|*|google-"
            },
            "promptPasswordFlag" : {
              "title" : "Prompt for password setting and activation code",
              "description" : "Users must set a password and complete the activation flow during
 dynamic profile creation.<br><br>If this is enabled, the user must set a password before the system
 creates an account dynamically and an activation code will be sent to the user's email address. The
 account will be created only if the password and activation code are properly set. <br />If this is
 disabled, the account will be created transparently without prompting the user.",
              "propertyOrder" : 1905,
              "required" : true,
              "type" : "boolean",
              "exampleValue" : ""
            },
            "attributeMapperConfiguration" : {
              "title" : "Attribute Mapper Configuration",
              "description" : "Mapping of OAuth attributes to local OpenAM attributes<br><br>Attribute
 configuration that will be used to map the user info obtained from the OAuth 2.0 Provider to the
```

```
 local user data store in the OpenAM.<br/><br/>Example: <code>OAuth2.0_attribute=local_attribute</
code>",
              "propertyOrder" : 1800,
              "required" : true,
              "items" : {
                "type" : "string"
              },
              "type" : "array",
              "exampleValue" : "given_name=givenName family_name=sn name=cn email=mail sub=uid"
            },
            "attributeMappingClasses" : {
              "title" : "Attribute Mapper",
              "description" : "Name of the class that implements the attribute
 mapping<br><br>This class maps the OAuth properties into OpenAM properties. A custom
 attribute mapper can be provided.<br/><br/>A custom attribute mapper must implement the
 <code>org.forgerock.openam.authentication.modules.common.mapping.AttributeMapper</code>
 interface.<br/>Provided implementations
 are:<ul><li>org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper</
li><li>org.forgerock.openam.authentication.modules.oidc.JwtAttributeMapper (can only be used when
 using the openid scope)</li></ul>String constructor parameters can be provided by appending <code>|</
code> separated values.",
              "propertyOrder" : 1700,
              "required" : true,
              "items" : {
                "type" : "string"
              },
              "type" : "array",
              "exampleValue" :
 "org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper|uid|google-"
            },
            "createAccount" : {
              "title" : "Create account if it does not exist",
              "description" : "If the OAuth2 account does not exist in the local OpenAM data store,
 an account will be created dynamically.<br><br>If this is enabled, the account mapper could create
 the account dynamically if there is no account mapped. Before creating the account, a dialog
 prompting for a password and asking for an activation code can be shown if the parameter \"Prompt
 for password setting and activation code\" is enabled.<br /><br />If this flag is not enabled, 3
 alternative options exist:<br/><br/><ol><li>The accounts need to have a user profile in the OpenAM
 User Data Store</li><li>The user does not have a user profile and the \"Ignore Profile\" is set in
 the Authentication Service of the realm.</li><li>The account is mapped to an anonymous account (see
 parameter \"Map to anonymous user\" and \"Anonymous User\")</li></ol>",
              "propertyOrder" : 1360,
              "required" : true,
              "type" : "boolean",
              "exampleValue" : ""
            },
            "accountProviderClass" : {
              "title" : "Account Provider",
              "description" : "Name of the class implementing the account provider.<br><br>This
 class is used by the module to find the account from the attributes mapped by the Account
 Mapper <code>org.forgerock.openam.authentication.modules.common.mapping.AccountProvider</code>
 interface.<br/>String constructor parameters can be provided by appending <code>|</code> separated
 values.",
              "propertyOrder" : 1400,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            },
            "mapToAnonymousUser" : {
```

```
              "title" : "Map to anonymous user",
              "description" : "Enabled anonymous user access to OpenAM for OAuth authenticated
 users<br><br>If selected, the authenticated users in the OAuth 2.0 Provider will be mapped to the
 anonymous user configured in the next parameter.<br/>If not selected the users authenticated will be
 mapped by the parameters configured in the account mapper.<br/><br/><i>NB </i>If <i>Create account if
 it does not exist</i> is enabled, that parameter takes precedence.",
              "propertyOrder" : 2000,
              "required" : true,
              "type" : "boolean",
              "exampleValue" : ""
            },
            "enableRegistrationService" : {
              "title" : "Use IDM as Registration Service",
              "description" : "Whether to use IDM as an external Registration Service to
 complete registration for new users.<br><br>IDM is called and passed these parameters:<br/><br/
><ul><li><code>clientToken</code>: Signed, encrypted JWT of the OAuth 2.0 authentication state.</
li><li><code>returnParams</code>: Encoded URL parameters, required to be returned to AM to resume
 authentication after registration in IDM is complete.</li></ul>",
              "propertyOrder" : 1350,
              "required" : true,
              "type" : "boolean",
              "exampleValue" : ""
            }
          }
        },
        "emailSettings" : {
          "type" : "object",
          "title" : "Email",
          "propertyOrder" : 2,
          "properties" : {
            "smtpSslEnabled" : {
              "title" : "SMTP SSL Enabled",
              "description" : "Tick this option if the SMTP Server provides SSL",
              "propertyOrder" : 1940,
              "required" : true,
              "type" : "boolean",
              "exampleValue" : ""
            },
            "smtpPassword" : {
              "title" : "SMTP User Password",
              "description" : "The Password of the SMTP User Name",
              "propertyOrder" : 1935,
              "required" : true,
              "type" : "string",
              "format" : "password",
              "exampleValue" : ""
            },
            "smtpUsername" : {
              "title" : "SMTP User Name",
              "description" : "If the SMTP Service requires authentication, configure the user name
 here",
              "propertyOrder" : 1930,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            },
            "emailAttribute" : {
              "title" : "Email attribute in the Response",
```

```
              "description" : "Attribute from the response used to send activation code
 emails.<br><br>The attribute in the response from the profile service of the Provider that contains
 the email address of the authenticated user. This address will be used to send an email with an
 activation code when the accounts are allowed to be created dynamically.",
              "propertyOrder" : 1910,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            },
            "emailGateway" : {
              "title" : "Mail Server Gateway implementation class",
              "description" : "The class used by the module to send
 email.<br><br>This class is used by the module to send email. A custom
 implementation can be provided.<br/><br/>The custom implementation must implement the
 <code>org.forgerock.openam.authentication.modules.oauth2.EmailGateway</code>",
              "propertyOrder" : 1915,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            },
            "smtpHost" : {
              "title" : "SMTP host",
              "description" : "The mail host that will be used by the Email Gateway implementation",
              "propertyOrder" : 1920,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            },
            "smtpFromAddress" : {
              "title" : "SMTP From address",
              "description" : "The email address on behalf of whom the messages will be sent",
              "propertyOrder" : 1945,
              "required" : true,
              "type" : "string",
              "exampleValue" : "info@forgerock.com"
            },
            "smtpPort" : {
              "title" : "SMTP port",
              "description" : "The TCP port that will be used by the SMTP gateway",
              "propertyOrder" : 1925,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            }
          }
        }
      },
      "type" : "object",
      "title" : "Realm Defaults"
    }
  }
}
```

SocialAuthOpenIDModule

Realm Operations

Resource path: `/realm-config/authentication/modules/authSocialOpenID`

Resource version: `1.0`

create

Usage:

```
am> create SocialAuthOpenIDModule --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "core" : {
      "type" : "object",
      "title" : "Core",
      "propertyOrder" : 0,
      "properties" : {
        "usesBasicAuth" : {
          "title" : "Use Basic Auth",
          "description" : "When enabled, the client will use basic auth for authenticating with  the
 social auth provider. Enabled by default.",
          "propertyOrder" : 1200,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "logoutServiceUrl" : {
          "title" : "OAuth 2.0 Provider Logout Service",
          "description" : "The URL of the Identity Provider's
 logout service.<br><br>To enable IdP logout, you must also add
 <code>org.forgerock.openam.authentication.modules.oauth2.OAuth2PostAuthnPlugin</code> to the
 <em>Authentication Post Processing Classes</em> setting. Navigate to Authentication > Settings > Post
 Authentication Processing.",
          "propertyOrder" : 2150,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
```

```
        "tokenEndpoint" : {
          "title" : "Access Token Endpoint URL",
          "description" : "OAuth access token endpoint URL<br><br>This is the URL endpoint for
 access token retrieval provided by the OAuth Identity Provider. Refer to the <a href=\"http://
tools.ietf.org/html/rfc6749#section-3.2\" target=\"_blank\">RFC 6749</a>, section 3.2",
          "propertyOrder" : 700,
          "required" : true,
          "type" : "string",
          "exampleValue" : "https://www.googleapis.com/oauth2/v4/token"
        },
        "clientId" : {
          "title" : "Client Id",
          "description" : "OAuth client_id parameter<br><br>For more information on the OAuth
 client_id parameter refer to the <a href=\"http://tools.ietf.org/html/rfc6749#section-2.3.1\" target=
\"_blank\">RFC 6749</a>, section 2.3.1",
          "propertyOrder" : 200,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "authorizeEndpoint" : {
          "title" : "Authentication Endpoint URL",
          "description" : "OAuth authentication endpoint URL<br><br>This is the URL endpoint for OAuth
 authentication provided by the OAuth Identity Provider",
          "propertyOrder" : 600,
          "required" : true,
          "type" : "string",
          "exampleValue" : "https://accounts.google.com/o/oauth2/v2/auth"
        },
        "issuerName" : {
          "title" : "Token Issuer",
          "description" : "Required when the 'openid' scope is included. Value must match the iss
 field in issued ID Token<br/>e.g. accounts.google.com<br><br>The issuer value MUST be provided when
 OAuth 2.0 Mix-Up Mitigation is enabled.",
          "propertyOrder" : 2700,
          "required" : true,
          "type" : "string",
          "exampleValue" : "https://accounts.google.com"
        },
        "authenticationLevel" : {
          "title" : "Authentication Level",
          "description" : "The authentication level associated with this module.<br><br>Each
 authentication module has an authentication level that can be used to indicate the level of security
 associated with the module; 0 is the lowest (and the default).",
          "propertyOrder" : 400,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "scopeDelimiter" : {
          "title" : "Scope Delimiter",
          "description" : "Delimiter used to separate scope values. Default value is space.",
          "propertyOrder" : 1000,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "provider" : {
          "title" : "Social Provider",
```

```
          "description" : "Social Provider for which this module is being setup.",
          "propertyOrder" : 100,
          "required" : true,
          "type" : "string",
          "exampleValue" : "Google"
        },
        "logoutBehaviour" : {
          "title" : "Logout Options",
          "description" : "Specify logout behavior.<br><br>The following options are available
 for logging out of the OAuth 2.0 Provider when the user logs out of AM:<br/><ul><li>prompt:
 Ask the user whether to log out from the OAuth 2.0 Provider</li><li>logout: Log out from
 the OAuth 2.0 Provider without asking the user</li><li>donotlogout: Do not log out the
 user from the OAuth 2.0 Provider</li></ul><br/>To enable IdP logout, you must also add
 <code>org.forgerock.openam.authentication.modules.oauth2.OAuth2PostAuthnPlugin</code> to the
 <em>Authentication Post Processing Classes</em> setting. Navigate to Authentication > Settings > Post
 Authentication Processing.",
          "propertyOrder" : 2155,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "scope" : {
          "title" : "Scope",
          "description" : "OAuth scope; list of user profile properties<br><br>According to the OAuth
 2.0 Authorization Framework, scope is a space-separated list of user profile attributes that the
 client application requires. The list depends on the permissions that the resource owner grants to
 the client application.<br/><br/> Some authorization servers use non-standard separators for scopes.
 For example, Facebook takes a comma-separated list.<br/><br/>",
          "propertyOrder" : 900,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "minItems" : 1,
          "type" : "array",
          "exampleValue" : "profile email openid"
        },
        "mixUpMitigation" : {
          "title" : "OAuth 2.0 Mix-Up Mitigation enabled",
          "description" : "Enables OAuth 2.0 mix-up mitigation<br><br>The authorization
 server must support the <a href=\"https://tools.ietf.org/html/draft-ietf-oauth-mix-up-
mitigation-01#section-3.1\">OAuth 2.0 Mix-Up Mitigation draft</a>, otherwise OpenAM will fail to
 validate responses from the authorization server. If only the OAuth 2.0 protocol is utilized, make
 sure that the accepted issuer value is set in the \"Token Issuer\" setting.",
          "propertyOrder" : 2800,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "subjectProperty" : {
          "title" : "Subject Property",
          "description" : "Property used to identify which attribute an auth server identifies a user
 by.",
          "propertyOrder" : 1100,
          "required" : true,
          "type" : "string",
          "exampleValue" : "sub"
        },
        "userInfoEndpoint" : {
```

```
          "title" : "User Profile Service URL",
          "description" : "User profile information URL<br><br>This URL endpoint provides user profile
information and is provided by the OAuth Identity Provider<br/><br/><i>NB </i>This URL should return
JSON objects in response",
          "propertyOrder" : 800,
          "required" : true,
          "type" : "string",
          "exampleValue" : "https://www.googleapis.com/oauth2/v3/userinfo"
        },
        "ssoProxyUrl" : {
          "title" : "Proxy URL",
          "description" : "The URL to the OpenAM OAuth proxy JSP<br><br>This URL should only be
changed from the default, if an external server is performing the GET to POST proxying. The default
is <code>/openam/oauth2c/OAuthProxy.jsp</code>",
          "propertyOrder" : 1300,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "clientSecret" : {
          "title" : "Client Secret",
          "description" : "OAuth client_secret parameter<br><br>For more information on the OAuth
client_secret parameter refer to the <a href=\"http://tools.ietf.org/html/rfc6749#section-2.3.1\"
target=\"_blank\">RFC 6749</a>, section 2.3.1",
          "propertyOrder" : 300,
          "required" : true,
          "type" : "string",
          "format" : "password",
          "exampleValue" : ""
        }
      }
    },
    "emailSettings" : {
      "type" : "object",
      "title" : "Email",
      "propertyOrder" : 3,
      "properties" : {
        "smtpUsername" : {
          "title" : "SMTP User Name",
          "description" : "If the SMTP Service requires authentication, configure the user name here",
          "propertyOrder" : 1930,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "smtpPassword" : {
          "title" : "SMTP User Password",
          "description" : "The Password of the SMTP User Name",
          "propertyOrder" : 1935,
          "required" : true,
          "type" : "string",
          "format" : "password",
          "exampleValue" : ""
        },
        "emailAttribute" : {
          "title" : "Email attribute in the Response",
          "description" : "Attribute from the response used to send activation code emails.<br><br>The
attribute in the response from the profile service of the Provider that contains the email address of
```

```
the authenticated user. This address will be used to send an email with an activation code when the
accounts are allowed to be created dynamically.",
         "propertyOrder" : 1910,
         "required" : true,
         "type" : "string",
         "exampleValue" : ""
       },
       "smtpHost" : {
         "title" : "SMTP host",
         "description" : "The mail host that will be used by the Email Gateway implementation",
         "propertyOrder" : 1920,
         "required" : true,
         "type" : "string",
         "exampleValue" : ""
       },
       "smtpPort" : {
         "title" : "SMTP port",
         "description" : "The TCP port that will be used by the SMTP gateway",
         "propertyOrder" : 1925,
         "required" : true,
         "type" : "string",
         "exampleValue" : ""
       },
       "smtpFromAddress" : {
         "title" : "SMTP From address",
         "description" : "The email address on behalf of whom the messages will be sent",
         "propertyOrder" : 1945,
         "required" : true,
         "type" : "string",
         "exampleValue" : "info@forgerock.com"
       },
       "emailGateway" : {
         "title" : "Mail Server Gateway implementation class",
         "description" : "The class used by the module to send email.<br><br>This class is used by
the module to send email. A custom implementation can be provided.<br/><br/>The custom implementation
must implement the <code>org.forgerock.openam.authentication.modules.oauth2.EmailGateway</code>",
         "propertyOrder" : 1915,
         "required" : true,
         "type" : "string",
         "exampleValue" : ""
       },
       "smtpSslEnabled" : {
         "title" : "SMTP SSL Enabled",
         "description" : "Tick this option if the SMTP Server provides SSL",
         "propertyOrder" : 1940,
         "required" : true,
         "type" : "boolean",
         "exampleValue" : ""
       }
     }
   },
   "accountProvisioning" : {
     "type" : "object",
     "title" : "Account Provisioning",
     "propertyOrder" : 2,
     "properties" : {
       "enableRegistrationService" : {
         "title" : "Use IDM as Registration Service",
```

```
          "description" : "Whether to use IDM as an external Registration Service to complete
 registration for new users.<br><br>IDM is called and passed these parameters:<br/><br/
><ul><li><code>clientToken</code>: Signed, encrypted JWT of the OAuth 2.0 authentication state.</
li><li><code>returnParams</code>: Encoded URL parameters, required to be returned to AM to resume
 authentication after registration in IDM is complete.</li></ul>",
          "propertyOrder" : 1350,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "attributeMapperConfiguration" : {
          "title" : "Attribute Mapper Configuration",
          "description" : "Mapping of OAuth attributes to local OpenAM attributes<br><br>Attribute
 configuration that will be used to map the user info obtained from the OAuth 2.0 Provider to the
 local user data store in the OpenAM.<br/><br/>Example: <code>OAuth2.0_attribute=local_attribute</
code>",
          "propertyOrder" : 1800,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : "given_name=givenName family_name=sn name=cn email=mail sub=uid"
        },
        "mapToAnonymousUser" : {
          "title" : "Map to anonymous user",
          "description" : "Enabled anonymous user access to OpenAM for OAuth authenticated
 users<br><br>If selected, the authenticated users in the OAuth 2.0 Provider will be mapped to the
 anonymous user configured in the next parameter.<br/>If not selected the users authenticated will be
 mapped by the parameters configured in the account mapper.<br/><br/><i>NB </i>If <i>Create account if
 it does not exist</i> is enabled, that parameter takes precedence.",
          "propertyOrder" : 2000,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "promptPasswordFlag" : {
          "title" : "Prompt for password setting and activation code",
          "description" : "Users must set a password and complete the activation flow during dynamic
 profile creation.<br><br>If this is enabled, the user must set a password before the system creates
 an account dynamically and an activation code will be sent to the user's email address. The account
 will be created only if the password and activation code are properly set. <br />If this is disabled,
 the account will be created transparently without prompting the user.",
          "propertyOrder" : 1905,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "attributeMappingClasses" : {
          "title" : "Attribute Mapper",
          "description" : "Name of the class that implements the attribute
 mapping<br><br>This class maps the OAuth properties into OpenAM properties. A custom
 attribute mapper can be provided.<br/><br/>A custom attribute mapper must implement the
 <code>org.forgerock.openam.authentication.modules.common.mapping.AttributeMapper</code>
 interface.<br/>Provided implementations
 are:<ul><li>org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper</
li><li>org.forgerock.openam.authentication.modules.oidc.JwtAttributeMapper (can only be used when
 using the openid scope)</li></ul>String constructor parameters can be provided by appending <code>|</
code> separated values.",
```

```
          "propertyOrder" : 1700,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" :
 "org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper|uid|google-"
        },
        "accountMapperConfiguration" : {
          "title" : "Account Mapper Configuration",
          "description" : "Mapping of OAuth account to local OpenAM account<br><br>Attribute
 configuration that will be used to map the account of the user authenticated in the OAuth 2.0
 Provider to the local data store in the OpenAM. Example: <code>OAuth2.0_attribute=local_attribute</
code>",
          "propertyOrder" : 1600,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : "sub=uid"
        },
        "accountMapperClass" : {
          "title" : "Account Mapper",
          "description" : "Name of the class implementing the attribute mapping for the
 account search.<br><br>This class is used by the module to map from the account information
 received from the OAuth Identity Provider into OpenAM.<br/><br/>The class must implement
 the <code>org.forgerock.openam.authentication.modules.common.mapping.AttributeMapper</code>
 interface.<br/>Provided implementations
 are:<ul><li>org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper</
li><li>org.forgerock.openam.authentication.modules.oidc.JwtAttributeMapper (can only be used when
 using the openid scope)</li></ul>String constructor parameters can be provided by appending <code>|</
code> separated values.",
          "propertyOrder" : 1500,
          "required" : true,
          "type" : "string",
          "exampleValue" :
 "org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper|*|google-"
        },
        "createAccount" : {
          "title" : "Create account if it does not exist",
          "description" : "If the OAuth2 account does not exist in the local OpenAM data store, an
 account will be created dynamically.<br><br>If this is enabled, the account mapper could create
 the account dynamically if there is no account mapped. Before creating the account, a dialog
 prompting for a password and asking for an activation code can be shown if the parameter \"Prompt
 for password setting and activation code\" is enabled.<br /><br />If this flag is not enabled, 3
 alternative options exist:<br/><br/><ol><li>The accounts need to have a user profile in the OpenAM
 User Data Store</li><li>The user does not have a user profile and the \"Ignore Profile\" is set in
 the Authentication Service of the realm.</li><li>The account is mapped to an anonymous account (see
 parameter \"Map to anonymous user\" and \"Anonymous User\")</li></ol>",
          "propertyOrder" : 1360,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "saveAttributesInSession" : {
          "title" : "Save attributes in the session",
```

```
          "description" : "If this option is enabled, the attributes configured in the attribute
 mapper will be saved into the OpenAM session",
          "propertyOrder" : 2400,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "accountProviderClass" : {
          "title" : "Account Provider",
          "description" : "Name of the class implementing the account provider.<br><br>This
 class is used by the module to find the account from the attributes mapped by the Account
 Mapper <code>org.forgerock.openam.authentication.modules.common.mapping.AccountProvider</code>
 interface.<br/>String constructor parameters can be provided by appending <code>|</code> separated
 values.",
          "propertyOrder" : 1400,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "anonymousUserName" : {
          "title" : "Anonymous User",
          "description" : "Username of the OpenAM anonymous user<br><br>The username of the user that
 will represent the anonymous user. This user account must already exist in the realm.",
          "propertyOrder" : 2100,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "openId" : {
      "type" : "object",
      "title" : "OpenID Connect",
      "propertyOrder" : 1,
      "properties" : {
        "cryptoContextType" : {
          "title" : "OpenID Connect validation configuration type",
          "description" : "Required when the 'openid' scope is included. Please select either 1. the
 issuer discovery url, 2. the issuer jwk url, or 3. the client_secret.",
          "propertyOrder" : 2500,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "cryptoContextValue" : {
          "title" : "OpenID Connect validation configuration value",
          "description" : "Required when the 'openid' scope is included. The discovery url, or jwk
 url, or the client_secret, corresponding to the selection above.<br><br>If discovery or jwk url
 entered, entry must be in valid url format, <br/>e.g. https://accounts.google.com/.well-known/openid-
configuration<br/><i>NB </i>If client_secret entered, entry is ignored and the value of the Client
 Secret is used.",
          "propertyOrder" : 2600,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    }
  }
```

```
}
```

delete

Usage:

```
am> delete SocialAuthOpenIDModule --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action SocialAuthOpenIDModule --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action SocialAuthOpenIDModule --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action SocialAuthOpenIDModule --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query SocialAuthOpenIDModule --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read SocialAuthOpenIDModule --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update SocialAuthOpenIDModule --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "core" : {
      "type" : "object",
      "title" : "Core",
      "propertyOrder" : 0,
      "properties" : {
        "usesBasicAuth" : {
          "title" : "Use Basic Auth",
          "description" : "When enabled, the client will use basic auth for authenticating with  the
 social auth provider. Enabled by default.",
          "propertyOrder" : 1200,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "logoutServiceUrl" : {
          "title" : "OAuth 2.0 Provider Logout Service",
          "description" : "The URL of the Identity Provider's
 logout service.<br><br>To enable IdP logout, you must also add
 <code>org.forgerock.openam.authentication.modules.oauth2.OAuth2PostAuthnPlugin</code> to the
```

```
 <em>Authentication Post Processing Classes</em> setting. Navigate to Authentication > Settings > Post
 Authentication Processing.",
          "propertyOrder" : 2150,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "tokenEndpoint" : {
          "title" : "Access Token Endpoint URL",
          "description" : "OAuth access token endpoint URL<br><br>This is the URL endpoint for
 access token retrieval provided by the OAuth Identity Provider. Refer to the <a href=\"http://
tools.ietf.org/html/rfc6749#section-3.2\" target=\"_blank\">RFC 6749</a>, section 3.2",
          "propertyOrder" : 700,
          "required" : true,
          "type" : "string",
          "exampleValue" : "https://www.googleapis.com/oauth2/v4/token"
        },
        "clientId" : {
          "title" : "Client Id",
          "description" : "OAuth client_id parameter<br><br>For more information on the OAuth
 client_id parameter refer to the <a href=\"http://tools.ietf.org/html/rfc6749#section-2.3.1\" target=
\"_blank\">RFC 6749</a>, section 2.3.1",
          "propertyOrder" : 200,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "authorizeEndpoint" : {
          "title" : "Authentication Endpoint URL",
          "description" : "OAuth authentication endpoint URL<br><br>This is the URL endpoint for OAuth
 authentication provided by the OAuth Identity Provider",
          "propertyOrder" : 600,
          "required" : true,
          "type" : "string",
          "exampleValue" : "https://accounts.google.com/o/oauth2/v2/auth"
        },
        "issuerName" : {
          "title" : "Token Issuer",
          "description" : "Required when the 'openid' scope is included. Value must match the iss
 field in issued ID Token<br/>e.g. accounts.google.com<br><br>The issuer value MUST be provided when
 OAuth 2.0 Mix-Up Mitigation is enabled.",
          "propertyOrder" : 2700,
          "required" : true,
          "type" : "string",
          "exampleValue" : "https://accounts.google.com"
        },
        "authenticationLevel" : {
          "title" : "Authentication Level",
          "description" : "The authentication level associated with this module.<br><br>Each
 authentication module has an authentication level that can be used to indicate the level of security
 associated with the module; 0 is the lowest (and the default).",
          "propertyOrder" : 400,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "scopeDelimiter" : {
          "title" : "Scope Delimiter",
          "description" : "Delimiter used to separate scope values. Default value is space.",
```

```
          "propertyOrder" : 1000,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "provider" : {
          "title" : "Social Provider",
          "description" : "Social Provider for which this module is being setup.",
          "propertyOrder" : 100,
          "required" : true,
          "type" : "string",
          "exampleValue" : "Google"
        },
        "logoutBehaviour" : {
          "title" : "Logout Options",
          "description" : "Specify logout behavior.<br><br>The following options are available
 for logging out of the OAuth 2.0 Provider when the user logs out of AM:<br/><ul><li>prompt:
 Ask the user whether to log out from the OAuth 2.0 Provider</li><li>logout: Log out from
 the OAuth 2.0 Provider without asking the user</li><li>donotlogout: Do not log out the
 user from the OAuth 2.0 Provider</li></ul><br/>To enable IdP logout, you must also add
 <code>org.forgerock.openam.authentication.modules.oauth2.OAuth2PostAuthnPlugin</code> to the
 <em>Authentication Post Processing Classes</em> setting. Navigate to Authentication > Settings > Post
 Authentication Processing.",
          "propertyOrder" : 2155,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "scope" : {
          "title" : "Scope",
          "description" : "OAuth scope; list of user profile properties<br><br>According to the OAuth
 2.0 Authorization Framework, scope is a space-separated list of user profile attributes that the
 client application requires. The list depends on the permissions that the resource owner grants to
 the client application.<br/><br/> Some authorization servers use non-standard separators for scopes.
 For example, Facebook takes a comma-separated list.<br/><br/>",
          "propertyOrder" : 900,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "minItems" : 1,
          "type" : "array",
          "exampleValue" : "profile email openid"
        },
        "mixUpMitigation" : {
          "title" : "OAuth 2.0 Mix-Up Mitigation enabled",
          "description" : "Enables OAuth 2.0 mix-up mitigation<br><br>The authorization
 server must support the <a href=\"https://tools.ietf.org/html/draft-ietf-oauth-mix-up-
mitigation-01#section-3.1\">OAuth 2.0 Mix-Up Mitigation draft</a>, otherwise OpenAM will fail to
 validate responses from the authorization server. If only the OAuth 2.0 protocol is utilized, make
 sure that the accepted issuer value is set in the \"Token Issuer\" setting.",
          "propertyOrder" : 2800,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "subjectProperty" : {
          "title" : "Subject Property",
```

```
          "description" : "Property used to identify which attribute an auth server identifies a user
by.",
          "propertyOrder" : 1100,
          "required" : true,
          "type" : "string",
          "exampleValue" : "sub"
        },
        "userInfoEndpoint" : {
          "title" : "User Profile Service URL",
          "description" : "User profile information URL<br><br>This URL endpoint provides user profile
information and is provided by the OAuth Identity Provider<br/><br/><i>NB </i>This URL should return
JSON objects in response",
          "propertyOrder" : 800,
          "required" : true,
          "type" : "string",
          "exampleValue" : "https://www.googleapis.com/oauth2/v3/userinfo"
        },
        "ssoProxyUrl" : {
          "title" : "Proxy URL",
          "description" : "The URL to the OpenAM OAuth proxy JSP<br><br>This URL should only be
changed from the default, if an external server is performing the GET to POST proxying. The default
is <code>/openam/oauth2c/OAuthProxy.jsp</code>",
          "propertyOrder" : 1300,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "clientSecret" : {
          "title" : "Client Secret",
          "description" : "OAuth client_secret parameter<br><br>For more information on the OAuth
client_secret parameter refer to the <a href=\"http://tools.ietf.org/html/rfc6749#section-2.3.1\"
target=\"_blank\">RFC 6749</a>, section 2.3.1",
          "propertyOrder" : 300,
          "required" : true,
          "type" : "string",
          "format" : "password",
          "exampleValue" : ""
        }
      }
    },
    "emailSettings" : {
      "type" : "object",
      "title" : "Email",
      "propertyOrder" : 3,
      "properties" : {
        "smtpUsername" : {
          "title" : "SMTP User Name",
          "description" : "If the SMTP Service requires authentication, configure the user name here",
          "propertyOrder" : 1930,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "smtpPassword" : {
          "title" : "SMTP User Password",
          "description" : "The Password of the SMTP User Name",
          "propertyOrder" : 1935,
          "required" : true,
          "type" : "string",
```

```
          "format" : "password",
          "exampleValue" : ""
        },
        "emailAttribute" : {
          "title" : "Email attribute in the Response",
          "description" : "Attribute from the response used to send activation code emails.<br><br>The
attribute in the response from the profile service of the Provider that contains the email address of
the authenticated user. This address will be used to send an email with an activation code when the
accounts are allowed to be created dynamically.",
          "propertyOrder" : 1910,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "smtpHost" : {
          "title" : "SMTP host",
          "description" : "The mail host that will be used by the Email Gateway implementation",
          "propertyOrder" : 1920,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "smtpPort" : {
          "title" : "SMTP port",
          "description" : "The TCP port that will be used by the SMTP gateway",
          "propertyOrder" : 1925,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "smtpFromAddress" : {
          "title" : "SMTP From address",
          "description" : "The email address on behalf of whom the messages will be sent",
          "propertyOrder" : 1945,
          "required" : true,
          "type" : "string",
          "exampleValue" : "info@forgerock.com"
        },
        "emailGateway" : {
          "title" : "Mail Server Gateway implementation class",
          "description" : "The class used by the module to send email.<br><br>This class is used by
the module to send email. A custom implementation can be provided.<br/><br/>The custom implementation
must implement the <code>org.forgerock.openam.authentication.modules.oauth2.EmailGateway</code>",
          "propertyOrder" : 1915,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "smtpSslEnabled" : {
          "title" : "SMTP SSL Enabled",
          "description" : "Tick this option if the SMTP Server provides SSL",
          "propertyOrder" : 1940,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        }
      }
    },
    "accountProvisioning" : {
```

```
      "type" : "object",
      "title" : "Account Provisioning",
      "propertyOrder" : 2,
      "properties" : {
        "enableRegistrationService" : {
          "title" : "Use IDM as Registration Service",
          "description" : "Whether to use IDM as an external Registration Service to complete
 registration for new users.<br><br>IDM is called and passed these parameters:<br/><br/
><ul><li><code>clientToken</code>: Signed, encrypted JWT of the OAuth 2.0 authentication state.</
li><li><code>returnParams</code>: Encoded URL parameters, required to be returned to AM to resume
 authentication after registration in IDM is complete.</li></ul>",
          "propertyOrder" : 1350,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "attributeMapperConfiguration" : {
          "title" : "Attribute Mapper Configuration",
          "description" : "Mapping of OAuth attributes to local OpenAM attributes<br><br>Attribute
 configuration that will be used to map the user info obtained from the OAuth 2.0 Provider to the
 local user data store in the OpenAM.<br/><br/>Example: <code>OAuth2.0_attribute=local_attribute</
code>",
          "propertyOrder" : 1800,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : "given_name=givenName family_name=sn name=cn email=mail sub=uid"
        },
        "mapToAnonymousUser" : {
          "title" : "Map to anonymous user",
          "description" : "Enabled anonymous user access to OpenAM for OAuth authenticated
 users<br><br>If selected, the authenticated users in the OAuth 2.0 Provider will be mapped to the
 anonymous user configured in the next parameter.<br/>If not selected the users authenticated will be
 mapped by the parameters configured in the account mapper.<br/><br/><i>NB </i>If <i>Create account if
 it does not exist</i> is enabled, that parameter takes precedence.",
          "propertyOrder" : 2000,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "promptPasswordFlag" : {
          "title" : "Prompt for password setting and activation code",
          "description" : "Users must set a password and complete the activation flow during dynamic
 profile creation.<br><br>If this is enabled, the user must set a password before the system creates
 an account dynamically and an activation code will be sent to the user's email address. The account
 will be created only if the password and activation code are properly set. <br />If this is disabled,
 the account will be created transparently without prompting the user.",
          "propertyOrder" : 1905,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "attributeMappingClasses" : {
          "title" : "Attribute Mapper",
          "description" : "Name of the class that implements the attribute
 mapping<br><br>This class maps the OAuth properties into OpenAM properties. A custom
 attribute mapper can be provided.<br/><br/>A custom attribute mapper must implement the
```

```
 <code>org.forgerock.openam.authentication.modules.common.mapping.AttributeMapper</code>
 interface.<br/>Provided implementations
 are:<ul><li>org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper</
li><li>org.forgerock.openam.authentication.modules.oidc.JwtAttributeMapper (can only be used when
 using the openid scope)</li></ul>String constructor parameters can be provided by appending <code>|</
code> separated values.",
          "propertyOrder" : 1700,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" :
 "org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper|uid|google-"
        },
        "accountMapperConfiguration" : {
          "title" : "Account Mapper Configuration",
          "description" : "Mapping of OAuth account to local OpenAM account<br><br>Attribute
 configuration that will be used to map the account of the user authenticated in the OAuth 2.0
 Provider to the local data store in the OpenAM. Example: <code>OAuth2.0_attribute=local_attribute</
code>",
          "propertyOrder" : 1600,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : "sub=uid"
        },
        "accountMapperClass" : {
          "title" : "Account Mapper",
          "description" : "Name of the class implementing the attribute mapping for the
 account search.<br><br>This class is used by the module to map from the account information
 received from the OAuth Identity Provider into OpenAM.<br/><br/>The class must implement
 the <code>org.forgerock.openam.authentication.modules.common.mapping.AttributeMapper</code>
 interface.<br/>Provided implementations
 are:<ul><li>org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper</
li><li>org.forgerock.openam.authentication.modules.oidc.JwtAttributeMapper (can only be used when
 using the openid scope)</li></ul>String constructor parameters can be provided by appending <code>|</
code> separated values.",
          "propertyOrder" : 1500,
          "required" : true,
          "type" : "string",
          "exampleValue" :
 "org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper|*|google-"
        },
        "createAccount" : {
          "title" : "Create account if it does not exist",
          "description" : "If the OAuth2 account does not exist in the local OpenAM data store, an
 account will be created dynamically.<br><br>If this is enabled, the account mapper could create
 the account dynamically if there is no account mapped. Before creating the account, a dialog
 prompting for a password and asking for an activation code can be shown if the parameter \"Prompt
 for password setting and activation code\" is enabled.<br /><br />If this flag is not enabled, 3
 alternative options exist:<br/><br/><ol><li>The accounts need to have a user profile in the OpenAM
 User Data Store</li><li>The user does not have a user profile and the \"Ignore Profile\" is set in
 the Authentication Service of the realm.</li><li>The account is mapped to an anonymous account (see
 parameter \"Map to anonymous user\" and \"Anonymous User\")</li></ol>",
          "propertyOrder" : 1360,
          "required" : true,
```

```
          "type" : "boolean",
          "exampleValue" : ""
        },
        "saveAttributesInSession" : {
          "title" : "Save attributes in the session",
          "description" : "If this option is enabled, the attributes configured in the attribute
 mapper will be saved into the OpenAM session",
          "propertyOrder" : 2400,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "accountProviderClass" : {
          "title" : "Account Provider",
          "description" : "Name of the class implementing the account provider.<br><br>This
 class is used by the module to find the account from the attributes mapped by the Account
 Mapper <code>org.forgerock.openam.authentication.modules.common.mapping.AccountProvider</code>
 interface.<br/>String constructor parameters can be provided by appending <code>|</code> separated
 values.",
          "propertyOrder" : 1400,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "anonymousUserName" : {
          "title" : "Anonymous User",
          "description" : "Username of the OpenAM anonymous user<br><br>The username of the user that
 will represent the anonymous user. This user account must already exist in the realm.",
          "propertyOrder" : 2100,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "openId" : {
      "type" : "object",
      "title" : "OpenID Connect",
      "propertyOrder" : 1,
      "properties" : {
        "cryptoContextType" : {
          "title" : "OpenID Connect validation configuration type",
          "description" : "Required when the 'openid' scope is included. Please select either 1. the
 issuer discovery url, 2. the issuer jwk url, or 3. the client_secret.",
          "propertyOrder" : 2500,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "cryptoContextValue" : {
          "title" : "OpenID Connect validation configuration value",
          "description" : "Required when the 'openid' scope is included. The discovery url, or jwk
 url, or the client_secret, corresponding to the selection above.<br><br>If discovery or jwk url
 entered, entry must be in valid url format, <br/>e.g. https://accounts.google.com/.well-known/openid-
configuration<br/><i>NB </i>If client_secret entered, entry is ignored and the value of the Client
 Secret is used.",
          "propertyOrder" : 2600,
          "required" : true,
          "type" : "string",
```

```
          "exampleValue" : ""
        }
      }
    }
  }
}
```

Global Operations

Resource path: `/global-config/authentication/modules/authSocialOpenID`

Resource version: `1.0`

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action SocialAuthOpenIDModule --global --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action SocialAuthOpenIDModule --global --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action SocialAuthOpenIDModule --global --actionName nextdescendents
```

read

Usage:

```
am> read SocialAuthOpenIDModule --global
```

update

Usage:

```
am> update SocialAuthOpenIDModule --global --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "defaults" : {
      "properties" : {
        "core" : {
          "type" : "object",
          "title" : "Core",
          "propertyOrder" : 0,
          "properties" : {
            "authenticationLevel" : {
              "title" : "Authentication Level",
              "description" : "The authentication level associated with this module.<br><br>Each
 authentication module has an authentication level that can be used to indicate the level of security
 associated with the module; 0 is the lowest (and the default).",
              "propertyOrder" : 400,
              "required" : true,
              "type" : "integer",
              "exampleValue" : ""
            },
            "usesBasicAuth" : {
              "title" : "Use Basic Auth",
              "description" : "When enabled, the client will use basic auth for authenticating with
 the social auth provider. Enabled by default.",
              "propertyOrder" : 1200,
              "required" : true,
              "type" : "boolean",
              "exampleValue" : ""
            },
            "provider" : {
              "title" : "Social Provider",
              "description" : "Social Provider for which this module is being setup.",
              "propertyOrder" : 100,
              "required" : true,
              "type" : "string",
              "exampleValue" : "Google"
            },
            "userInfoEndpoint" : {
              "title" : "User Profile Service URL",
              "description" : "User profile information URL<br><br>This URL endpoint provides user
 profile information and is provided by the OAuth Identity Provider<br/><br/><i>NB </i>This URL should
 return JSON objects in response",
              "propertyOrder" : 800,
              "required" : true,
              "type" : "string",
              "exampleValue" : "https://www.googleapis.com/oauth2/v3/userinfo"
            },
            "authorizeEndpoint" : {
              "title" : "Authentication Endpoint URL",
```

```
              "description" : "OAuth authentication endpoint URL<br><br>This is the URL endpoint for
 OAuth authentication provided by the OAuth Identity Provider",
              "propertyOrder" : 600,
              "required" : true,
              "type" : "string",
              "exampleValue" : "https://accounts.google.com/o/oauth2/v2/auth"
            },
            "issuerName" : {
              "title" : "Token Issuer",
              "description" : "Required when the 'openid' scope is included. Value must match the iss
 field in issued ID Token<br/>e.g. accounts.google.com<br><br>The issuer value MUST be provided when
 OAuth 2.0 Mix-Up Mitigation is enabled.",
              "propertyOrder" : 2700,
              "required" : true,
              "type" : "string",
              "exampleValue" : "https://accounts.google.com"
            },
            "logoutBehaviour" : {
              "title" : "Logout Options",
              "description" : "Specify logout behavior.<br><br>The following options are
 available for logging out of the OAuth 2.0 Provider when the user logs out of AM:<br/
><ul><li>prompt: Ask the user whether to log out from the OAuth 2.0 Provider</li><li>logout:
 Log out from the OAuth 2.0 Provider without asking the user</li><li>donotlogout: Do not log
 out the user from the OAuth 2.0 Provider</li></ul><br/>To enable IdP logout, you must also add
 <code>org.forgerock.openam.authentication.modules.oauth2.OAuth2PostAuthnPlugin</code> to the
 <em>Authentication Post Processing Classes</em> setting. Navigate to Authentication > Settings > Post
 Authentication Processing.",
              "propertyOrder" : 2155,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            },
            "ssoProxyUrl" : {
              "title" : "Proxy URL",
              "description" : "The URL to the OpenAM OAuth proxy JSP<br><br>This URL should only be
 changed from the default, if an external server is performing the GET to POST proxying. The default
 is <code>/openam/oauth2c/OAuthProxy.jsp</code>",
              "propertyOrder" : 1300,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            },
            "logoutServiceUrl" : {
              "title" : "OAuth 2.0 Provider Logout Service",
              "description" : "The URL of the Identity Provider's
 logout service.<br><br>To enable IdP logout, you must also add
 <code>org.forgerock.openam.authentication.modules.oauth2.OAuth2PostAuthnPlugin</code> to the
 <em>Authentication Post Processing Classes</em> setting. Navigate to Authentication > Settings > Post
 Authentication Processing.",
              "propertyOrder" : 2150,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            },
            "clientId" : {
              "title" : "Client Id",
              "description" : "OAuth client_id parameter<br><br>For more information on the OAuth
 client_id parameter refer to the <a href=\"http://tools.ietf.org/html/rfc6749#section-2.3.1\" target=
\"_blank\">RFC 6749</a>, section 2.3.1",
```

```
              "propertyOrder" : 200,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            },
            "scopeDelimiter" : {
              "title" : "Scope Delimiter",
              "description" : "Delimiter used to separate scope values. Default value is space.",
              "propertyOrder" : 1000,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            },
            "subjectProperty" : {
              "title" : "Subject Property",
              "description" : "Property used to identify which attribute an auth server identifies a
 user by.",
              "propertyOrder" : 1100,
              "required" : true,
              "type" : "string",
              "exampleValue" : "sub"
            },
            "scope" : {
              "title" : "Scope",
              "description" : "OAuth scope; list of user profile properties<br><br>According to the
 OAuth 2.0 Authorization Framework, scope is a space-separated list of user profile attributes that
 the client application requires. The list depends on the permissions that the resource owner grants
 to the client application.<br/><br/> Some authorization servers use non-standard separators for
 scopes. For example, Facebook takes a comma-separated list.<br/><br/>",
              "propertyOrder" : 900,
              "required" : true,
              "items" : {
                "type" : "string"
              },
              "type" : "array",
              "exampleValue" : "profile email openid"
            },
            "tokenEndpoint" : {
              "title" : "Access Token Endpoint URL",
              "description" : "OAuth access token endpoint URL<br><br>This is the URL endpoint for
 access token retrieval provided by the OAuth Identity Provider. Refer to the <a href=\"http://
tools.ietf.org/html/rfc6749#section-3.2\" target=\"_blank\">RFC 6749</a>, section 3.2",
              "propertyOrder" : 700,
              "required" : true,
              "type" : "string",
              "exampleValue" : "https://www.googleapis.com/oauth2/v4/token"
            },
            "clientSecret" : {
              "title" : "Client Secret",
              "description" : "OAuth client_secret parameter<br><br>For more information on the OAuth
 client_secret parameter refer to the <a href=\"http://tools.ietf.org/html/rfc6749#section-2.3.1\"
 target=\"_blank\">RFC 6749</a>, section 2.3.1",
              "propertyOrder" : 300,
              "required" : true,
              "type" : "string",
              "format" : "password",
              "exampleValue" : ""
            },
            "mixUpMitigation" : {
```

```
              "title" : "OAuth 2.0 Mix-Up Mitigation enabled",
              "description" : "Enables OAuth 2.0 mix-up mitigation<br><br>The authorization
 server must support the <a href=\"https://tools.ietf.org/html/draft-ietf-oauth-mix-up-
mitigation-01#section-3.1\">OAuth 2.0 Mix-Up Mitigation draft</a>, otherwise OpenAM will fail to
 validate responses from the authorization server. If only the OAuth 2.0 protocol is utilized, make
 sure that the accepted issuer value is set in the \"Token Issuer\" setting.",
              "propertyOrder" : 2800,
              "required" : true,
              "type" : "boolean",
              "exampleValue" : ""
            }
          }
        },
        "accountProvisioning" : {
          "type" : "object",
          "title" : "Account Provisioning",
          "propertyOrder" : 2,
          "properties" : {
            "createAccount" : {
              "title" : "Create account if it does not exist",
              "description" : "If the OAuth2 account does not exist in the local OpenAM data store,
 an account will be created dynamically.<br><br>If this is enabled, the account mapper could create
 the account dynamically if there is no account mapped. Before creating the account, a dialog
 prompting for a password and asking for an activation code can be shown if the parameter \"Prompt
 for password setting and activation code\" is enabled.<br /><br />If this flag is not enabled, 3
 alternative options exist:<br/><br/><ol><li>The accounts need to have a user profile in the OpenAM
 User Data Store</li><li>The user does not have a user profile and the \"Ignore Profile\" is set in
 the Authentication Service of the realm.</li><li>The account is mapped to an anonymous account (see
 parameter \"Map to anonymous user\" and \"Anonymous User\")</li></ol>",
              "propertyOrder" : 1360,
              "required" : true,
              "type" : "boolean",
              "exampleValue" : ""
            },
            "accountMapperConfiguration" : {
              "title" : "Account Mapper Configuration",
              "description" : "Mapping of OAuth account to local OpenAM account<br><br>Attribute
 configuration that will be used to map the account of the user authenticated in the OAuth 2.0
 Provider to the local data store in the OpenAM. Example: <code>OAuth2.0_attribute=local_attribute</
code>",
              "propertyOrder" : 1600,
              "required" : true,
              "items" : {
                "type" : "string"
              },
              "type" : "array",
              "exampleValue" : "sub=uid"
            },
            "enableRegistrationService" : {
              "title" : "Use IDM as Registration Service",
              "description" : "Whether to use IDM as an external Registration Service to
 complete registration for new users.<br><br>IDM is called and passed these parameters:<br/><br/
><ul><li><code>clientToken</code>: Signed, encrypted JWT of the OAuth 2.0 authentication state.</
li><li><code>returnParams</code>: Encoded URL parameters, required to be returned to AM to resume
 authentication after registration in IDM is complete.</li></ul>",
              "propertyOrder" : 1350,
              "required" : true,
              "type" : "boolean",
              "exampleValue" : ""
```

```
            },
            "accountMapperClass" : {
              "title" : "Account Mapper",
              "description" : "Name of the class implementing the attribute mapping for the
 account search.<br><br>This class is used by the module to map from the account information
 received from the OAuth Identity Provider into OpenAM.<br/><br/>The class must implement
 the <code>org.forgerock.openam.authentication.modules.common.mapping.AttributeMapper</code>
 interface.<br/>Provided implementations
 are:<ul><li>org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper</
li><li>org.forgerock.openam.authentication.modules.oidc.JwtAttributeMapper (can only be used when
 using the openid scope)</li></ul>String constructor parameters can be provided by appending <code>|</
code> separated values.",
              "propertyOrder" : 1500,
              "required" : true,
              "type" : "string",
              "exampleValue" :
 "org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper|*|google-"
            },
            "accountProviderClass" : {
              "title" : "Account Provider",
              "description" : "Name of the class implementing the account provider.<br><br>This
 class is used by the module to find the account from the attributes mapped by the Account
 Mapper <code>org.forgerock.openam.authentication.modules.common.mapping.AccountProvider</code>
 interface.<br/>String constructor parameters can be provided by appending <code>|</code> separated
 values.",
              "propertyOrder" : 1400,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            },
            "promptPasswordFlag" : {
              "title" : "Prompt for password setting and activation code",
              "description" : "Users must set a password and complete the activation flow during
 dynamic profile creation.<br><br>If this is enabled, the user must set a password before the system
 creates an account dynamically and an activation code will be sent to the user's email address. The
 account will be created only if the password and activation code are properly set. <br />If this is
 disabled, the account will be created transparently without prompting the user.",
              "propertyOrder" : 1905,
              "required" : true,
              "type" : "boolean",
              "exampleValue" : ""
            },
            "attributeMappingClasses" : {
              "title" : "Attribute Mapper",
              "description" : "Name of the class that implements the attribute
 mapping<br><br>This class maps the OAuth properties into OpenAM properties. A custom
 attribute mapper can be provided.<br/><br/>A custom attribute mapper must implement the
 <code>org.forgerock.openam.authentication.modules.common.mapping.AttributeMapper</code>
 interface.<br/>Provided implementations
 are:<ul><li>org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper</
li><li>org.forgerock.openam.authentication.modules.oidc.JwtAttributeMapper (can only be used when
 using the openid scope)</li></ul>String constructor parameters can be provided by appending <code>|</
code> separated values.",
              "propertyOrder" : 1700,
              "required" : true,
              "items" : {
                "type" : "string"
              },
              "type" : "array",
```

```
              "exampleValue" :
 "org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper|uid|google-"
            },
            "saveAttributesInSession" : {
              "title" : "Save attributes in the session",
              "description" : "If this option is enabled, the attributes configured in the attribute
 mapper will be saved into the OpenAM session",
              "propertyOrder" : 2400,
              "required" : true,
              "type" : "boolean",
              "exampleValue" : ""
            },
            "anonymousUserName" : {
              "title" : "Anonymous User",
              "description" : "Username of the OpenAM anonymous user<br><br>The username of the user
 that will represent the anonymous user. This user account must already exist in the realm.",
              "propertyOrder" : 2100,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            },
            "attributeMapperConfiguration" : {
              "title" : "Attribute Mapper Configuration",
              "description" : "Mapping of OAuth attributes to local OpenAM attributes<br><br>Attribute
 configuration that will be used to map the user info obtained from the OAuth 2.0 Provider to the
 local user data store in the OpenAM.<br/><br/>Example: <code>OAuth2.0_attribute=local_attribute</
code>",
              "propertyOrder" : 1800,
              "required" : true,
              "items" : {
                "type" : "string"
              },
              "type" : "array",
              "exampleValue" : "given_name=givenName family_name=sn name=cn email=mail sub=uid"
            },
            "mapToAnonymousUser" : {
              "title" : "Map to anonymous user",
              "description" : "Enabled anonymous user access to OpenAM for OAuth authenticated
 users<br><br>If selected, the authenticated users in the OAuth 2.0 Provider will be mapped to the
 anonymous user configured in the next parameter.<br/>If not selected the users authenticated will be
 mapped by the parameters configured in the account mapper.<br/><br/><i>NB </i>If <i>Create account if
 it does not exist</i> is enabled, that parameter takes precedence.",
              "propertyOrder" : 2000,
              "required" : true,
              "type" : "boolean",
              "exampleValue" : ""
            }
          }
        },
        "emailSettings" : {
          "type" : "object",
          "title" : "Email",
          "propertyOrder" : 3,
          "properties" : {
            "smtpUsername" : {
              "title" : "SMTP User Name",
              "description" : "If the SMTP Service requires authentication, configure the user name
 here",
              "propertyOrder" : 1930,
```

```
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            },
            "smtpPassword" : {
              "title" : "SMTP User Password",
              "description" : "The Password of the SMTP User Name",
              "propertyOrder" : 1935,
              "required" : true,
              "type" : "string",
              "format" : "password",
              "exampleValue" : ""
            },
            "smtpFromAddress" : {
              "title" : "SMTP From address",
              "description" : "The email address on behalf of whom the messages will be sent",
              "propertyOrder" : 1945,
              "required" : true,
              "type" : "string",
              "exampleValue" : "info@forgerock.com"
            },
            "smtpHost" : {
              "title" : "SMTP host",
              "description" : "The mail host that will be used by the Email Gateway implementation",
              "propertyOrder" : 1920,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            },
            "smtpSslEnabled" : {
              "title" : "SMTP SSL Enabled",
              "description" : "Tick this option if the SMTP Server provides SSL",
              "propertyOrder" : 1940,
              "required" : true,
              "type" : "boolean",
              "exampleValue" : ""
            },
            "smtpPort" : {
              "title" : "SMTP port",
              "description" : "The TCP port that will be used by the SMTP gateway",
              "propertyOrder" : 1925,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            },
            "emailAttribute" : {
              "title" : "Email attribute in the Response",
              "description" : "Attribute from the response used to send activation code
emails.<br><br>The attribute in the response from the profile service of the Provider that contains
the email address of the authenticated user. This address will be used to send an email with an
activation code when the accounts are allowed to be created dynamically.",
              "propertyOrder" : 1910,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            },
            "emailGateway" : {
              "title" : "Mail Server Gateway implementation class",
```

```
              "description" : "The class used by the module to send
 email.<br><br>This class is used by the module to send email. A custom
 implementation can be provided.<br/><br/>The custom implementation must implement the
 <code>org.forgerock.openam.authentication.modules.oauth2.EmailGateway</code>",
              "propertyOrder" : 1915,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            }
          }
        },
        "openId" : {
          "type" : "object",
          "title" : "OpenID Connect",
          "propertyOrder" : 1,
          "properties" : {
            "cryptoContextType" : {
              "title" : "OpenID Connect validation configuration type",
              "description" : "Required when the 'openid' scope is included. Please select either 1.
 the issuer discovery url, 2. the issuer jwk url, or 3. the client_secret.",
              "propertyOrder" : 2500,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            },
            "cryptoContextValue" : {
              "title" : "OpenID Connect validation configuration value",
              "description" : "Required when the 'openid' scope is included. The discovery url, or
 jwk url, or the client_secret, corresponding to the selection above.<br><br>If discovery or jwk url
 entered, entry must be in valid url format, <br/>e.g. https://accounts.google.com/.well-known/openid-
configuration<br/><i>NB </i>If client_secret entered, entry is ignored and the value of the Client
 Secret is used.",
              "propertyOrder" : 2600,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            }
          }
        }
      },
      "type" : "object",
      "title" : "Realm Defaults"
    }
  }
}
```


SocialAuthTwitterModule

Realm Operations

Resource path: `/realm-config/authentication/modules/authSocialTwitter`

Resource version: `1.0`

create

Usage:

```
am> create SocialAuthTwitterModule --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "core" : {
      "type" : "object",
      "title" : "Core",
      "propertyOrder" : 0,
      "properties" : {
        "clientId" : {
          "title" : "Client Id",
          "description" : "OAuth client_id parameter<br><br>For more information on the OAuth
 client_id parameter refer to the <a href=\"http://tools.ietf.org/html/rfc6749#section-2.3.1\" target=
\"_blank\">RFC 6749</a>, section 2.3.1",
          "propertyOrder" : 400,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "tokenEndpoint" : {
          "title" : "Access Token Endpoint URL",
          "description" : "OAuth access token endpoint URL<br><br>This is the URL endpoint for
 access token retrieval provided by the OAuth Identity Provider. Refer to the <a href=\"http://
tools.ietf.org/html/rfc6749#section-3.2\" target=\"_blank\">RFC 6749</a>, section 3.2",
          "propertyOrder" : 700,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "requestTokenEndpoint" : {
          "title" : "Request Token Endpoint URL",
          "description" : "OAuth request token endpoint URL<br><br>This is the URL endpoint for OAuth
 request token provided by the OAuth Identity Provider",
          "propertyOrder" : 600,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "userInfoEndpoint" : {
          "title" : "User Profile Service URL",
          "description" : "User profile information URL<br><br>This URL endpoint provides user profile
 information and is provided by the OAuth Identity Provider<br/><br/><i>NB </i>This URL should return
 JSON objects in response",
```

```
          "propertyOrder" : 800,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "ssoProxyUrl" : {
          "title" : "Proxy URL",
          "description" : "The URL to the OpenAM OAuth proxy JSP<br><br>This URL should only be
changed from the default, if an external server is performing the GET to POST proxying. The default
is <code>/openam/oauth2c/OAuthProxy.jsp</code>",
          "propertyOrder" : 1300,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "clientSecret" : {
          "title" : "Client Secret",
          "description" : "OAuth client_secret parameter<br><br>For more information on the OAuth
client_secret parameter refer to the <a href=\"http://tools.ietf.org/html/rfc6749#section-2.3.1\"
target=\"_blank\">RFC 6749</a>, section 2.3.1",
          "propertyOrder" : 500,
          "required" : true,
          "type" : "string",
          "format" : "password",
          "exampleValue" : ""
        },
        "subjectProperty" : {
          "title" : "Subject Property",
          "description" : "Property used to identify which attribute an auth server identifies a user
by.",
          "propertyOrder" : 1100,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "provider" : {
          "title" : "Social Provider",
          "description" : "Social Provider for which this module is being setup.",
          "propertyOrder" : 200,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "authenticationLevel" : {
          "title" : "Authentication Level",
          "description" : "The authentication level associated with this module.<br><br>Each
authentication module has an authentication level that can be used to indicate the level of security
associated with the module; 0 is the lowest (and the default).",
          "propertyOrder" : 100,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "authorizeEndpoint" : {
          "title" : "Authentication Endpoint URL",
          "description" : "OAuth authentication endpoint URL<br><br>This is the URL endpoint for OAuth
authentication provided by the OAuth Identity Provider",
          "propertyOrder" : 600,
          "required" : true,
```

```
          "type" : "string",
          "exampleValue" : ""
        },
        "usesBasicAuth" : {
          "title" : "Use Basic Auth",
          "description" : "When enabled, the client will use basic auth for authenticating with  the
social auth provider. Enabled by default.",
          "propertyOrder" : 1200,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        }
      }
    },
    "accountProvisioning" : {
      "type" : "object",
      "title" : "Account Provisioning",
      "propertyOrder" : 1,
      "properties" : {
        "accountProviderClass" : {
          "title" : "Account Provider",
          "description" : "Name of the class implementing the account provider.<br><br>This
class is used by the module to find the account from the attributes mapped by the Account
Mapper <code>org.forgerock.openam.authentication.modules.common.mapping.AccountProvider</code>
interface.<br/>String constructor parameters can be provided by appending <code>|</code> separated
values.",
          "propertyOrder" : 1400,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "mapToAnonymousUser" : {
          "title" : "Map to anonymous user",
          "description" : "Enabled anonymous user access to OpenAM for OAuth authenticated
users<br><br>If selected, the authenticated users in the OAuth 2.0 Provider will be mapped to the
anonymous user configured in the next parameter.<br/>If not selected the users authenticated will be
mapped by the parameters configured in the account mapper.<br/><br/><i>NB </i>If <i>Create account if
it does not exist</i> is enabled, that parameter takes precedence.",
          "propertyOrder" : 2000,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "anonymousUserName" : {
          "title" : "Anonymous User",
          "description" : "Username of the OpenAM anonymous user<br><br>The username of the user that
will represent the anonymous user. This user account must already exist in the realm.",
          "propertyOrder" : 2100,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "attributeMappingClasses" : {
          "title" : "Attribute Mapper",
          "description" : "Name of the class that implements the attribute
mapping<br><br>This class maps the OAuth properties into OpenAM properties. A custom
attribute mapper can be provided.<br/><br/>A custom attribute mapper must implement the
<code>org.forgerock.openam.authentication.modules.common.mapping.AttributeMapper</code>
interface.<br/>Provided implementations
```

```
 are:<ul><li>org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper</
li><li>org.forgerock.openam.authentication.modules.oidc.JwtAttributeMapper (can only be used when
 using the openid scope)</li></ul>String constructor parameters can be provided by appending <code>|</
code> separated values.",
          "propertyOrder" : 1700,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "attributeMapperConfiguration" : {
          "title" : "Attribute Mapper Configuration",
          "description" : "Mapping of OAuth attributes to local OpenAM attributes<br><br>Attribute
 configuration that will be used to map the user info obtained from the OAuth 2.0 Provider to the
 local user data store in the OpenAM.<br/><br/>Example: <code>OAuth2.0_attribute=local_attribute</
code>",
          "propertyOrder" : 1800,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "accountMapperConfiguration" : {
          "title" : "Account Mapper Configuration",
          "description" : "Mapping of OAuth account to local OpenAM account<br><br>Attribute
 configuration that will be used to map the account of the user authenticated in the OAuth 2.0
 Provider to the local data store in the OpenAM. Example: <code>OAuth2.0_attribute=local_attribute</
code>",
          "propertyOrder" : 1600,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "accountMapperClass" : {
          "title" : "Account Mapper",
          "description" : "Name of the class implementing the attribute mapping for the
 account search.<br><br>This class is used by the module to map from the account information
 received from the OAuth Identity Provider into OpenAM.<br/><br/>The class must implement
 the <code>org.forgerock.openam.authentication.modules.common.mapping.AttributeMapper</code>
 interface.<br/>Provided implementations
 are:<ul><li>org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper</
li><li>org.forgerock.openam.authentication.modules.oidc.JwtAttributeMapper (can only be used when
 using the openid scope)</li></ul>String constructor parameters can be provided by appending <code>|</
code> separated values.",
          "propertyOrder" : 1500,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "enableRegistrationService" : {
          "title" : "Use IDM as Registration Service",
```

```
          "description" : "Whether to use IDM as an external Registration Service to complete
 registration for new users.<br><br>IDM is called and passed these parameters:<br/><br/
><ul><li><code>clientToken</code>: Signed, encrypted JWT of the OAuth 2.0 authentication state.</
li><li><code>returnParams</code>: Encoded URL parameters, required to be returned to AM to resume
 authentication after registration in IDM is complete.</li></ul>",
          "propertyOrder" : 1350,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "createAccount" : {
          "title" : "Create account if it does not exist",
          "description" : "If the OAuth2 account does not exist in the local OpenAM data store, an
 account will be created dynamically.<br><br>If this is enabled, the account mapper could create
 the account dynamically if there is no account mapped. Before creating the account, a dialog
 prompting for a password and asking for an activation code can be shown if the parameter \"Prompt
 for password setting and activation code\" is enabled.<br /><br />If this flag is not enabled, 3
 alternative options exist:<br/><br/><ol><li>The accounts need to have a user profile in the OpenAM
 User Data Store</li><li>The user does not have a user profile and the \"Ignore Profile\" is set in
 the Authentication Service of the realm.</li><li>The account is mapped to an anonymous account (see
 parameter \"Map to anonymous user\" and \"Anonymous User\")</li></ol>",
          "propertyOrder" : 1360,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "saveAttributesInSession" : {
          "title" : "Save attributes in the session",
          "description" : "If this option is enabled, the attributes configured in the attribute
 mapper will be saved into the OpenAM session",
          "propertyOrder" : 2400,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        }
      }
    }
  }
}
```

delete

Usage:

```
am> delete SocialAuthTwitterModule --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action SocialAuthTwitterModule --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action SocialAuthTwitterModule --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action SocialAuthTwitterModule --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query SocialAuthTwitterModule --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read SocialAuthTwitterModule --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update SocialAuthTwitterModule --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "core" : {
      "type" : "object",
      "title" : "Core",
      "propertyOrder" : 0,
      "properties" : {
        "clientId" : {
          "title" : "Client Id",
          "description" : "OAuth client_id parameter<br><br>For more information on the OAuth
 client_id parameter refer to the <a href=\"http://tools.ietf.org/html/rfc6749#section-2.3.1\" target=
\"_blank\">RFC 6749</a>, section 2.3.1",
          "propertyOrder" : 400,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "tokenEndpoint" : {
          "title" : "Access Token Endpoint URL",
          "description" : "OAuth access token endpoint URL<br><br>This is the URL endpoint for
 access token retrieval provided by the OAuth Identity Provider. Refer to the <a href=\"http://
tools.ietf.org/html/rfc6749#section-3.2\" target=\"_blank\">RFC 6749</a>, section 3.2",
          "propertyOrder" : 700,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "requestTokenEndpoint" : {
          "title" : "Request Token Endpoint URL",
          "description" : "OAuth request token endpoint URL<br><br>This is the URL endpoint for OAuth
 request token provided by the OAuth Identity Provider",
          "propertyOrder" : 600,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "userInfoEndpoint" : {
          "title" : "User Profile Service URL",
          "description" : "User profile information URL<br><br>This URL endpoint provides user profile
 information and is provided by the OAuth Identity Provider<br/><br/><i>NB </i>This URL should return
 JSON objects in response",
```

```
          "propertyOrder" : 800,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "ssoProxyUrl" : {
          "title" : "Proxy URL",
          "description" : "The URL to the OpenAM OAuth proxy JSP<br><br>This URL should only be
changed from the default, if an external server is performing the GET to POST proxying. The default
is <code>/openam/oauth2c/OAuthProxy.jsp</code>",
          "propertyOrder" : 1300,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "clientSecret" : {
          "title" : "Client Secret",
          "description" : "OAuth client_secret parameter<br><br>For more information on the OAuth
client_secret parameter refer to the <a href=\"http://tools.ietf.org/html/rfc6749#section-2.3.1\"
target=\"_blank\">RFC 6749</a>, section 2.3.1",
          "propertyOrder" : 500,
          "required" : true,
          "type" : "string",
          "format" : "password",
          "exampleValue" : ""
        },
        "subjectProperty" : {
          "title" : "Subject Property",
          "description" : "Property used to identify which attribute an auth server identifies a user
by.",
          "propertyOrder" : 1100,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "provider" : {
          "title" : "Social Provider",
          "description" : "Social Provider for which this module is being setup.",
          "propertyOrder" : 200,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "authenticationLevel" : {
          "title" : "Authentication Level",
          "description" : "The authentication level associated with this module.<br><br>Each
authentication module has an authentication level that can be used to indicate the level of security
associated with the module; 0 is the lowest (and the default).",
          "propertyOrder" : 100,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "authorizeEndpoint" : {
          "title" : "Authentication Endpoint URL",
          "description" : "OAuth authentication endpoint URL<br><br>This is the URL endpoint for OAuth
authentication provided by the OAuth Identity Provider",
          "propertyOrder" : 600,
          "required" : true,
```

```
          "type" : "string",
          "exampleValue" : ""
        },
        "usesBasicAuth" : {
          "title" : "Use Basic Auth",
          "description" : "When enabled, the client will use basic auth for authenticating with  the
social auth provider. Enabled by default.",
          "propertyOrder" : 1200,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        }
      }
    },
    "accountProvisioning" : {
      "type" : "object",
      "title" : "Account Provisioning",
      "propertyOrder" : 1,
      "properties" : {
        "accountProviderClass" : {
          "title" : "Account Provider",
          "description" : "Name of the class implementing the account provider.<br><br>This
class is used by the module to find the account from the attributes mapped by the Account
Mapper <code>org.forgerock.openam.authentication.modules.common.mapping.AccountProvider</code>
interface.<br/>String constructor parameters can be provided by appending <code>|</code> separated
values.",
          "propertyOrder" : 1400,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "mapToAnonymousUser" : {
          "title" : "Map to anonymous user",
          "description" : "Enabled anonymous user access to OpenAM for OAuth authenticated
users<br><br>If selected, the authenticated users in the OAuth 2.0 Provider will be mapped to the
anonymous user configured in the next parameter.<br/>If not selected the users authenticated will be
mapped by the parameters configured in the account mapper.<br/><br/><i>NB </i>If <i>Create account if
it does not exist</i> is enabled, that parameter takes precedence.",
          "propertyOrder" : 2000,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "anonymousUserName" : {
          "title" : "Anonymous User",
          "description" : "Username of the OpenAM anonymous user<br><br>The username of the user that
will represent the anonymous user. This user account must already exist in the realm.",
          "propertyOrder" : 2100,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "attributeMappingClasses" : {
          "title" : "Attribute Mapper",
          "description" : "Name of the class that implements the attribute
mapping<br><br>This class maps the OAuth properties into OpenAM properties. A custom
attribute mapper can be provided.<br/><br/>A custom attribute mapper must implement the
<code>org.forgerock.openam.authentication.modules.common.mapping.AttributeMapper</code>
interface.<br/>Provided implementations
```

```
 are:<ul><li>org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper</
li><li>org.forgerock.openam.authentication.modules.oidc.JwtAttributeMapper (can only be used when
 using the openid scope)</li></ul>String constructor parameters can be provided by appending <code>|</
code> separated values.",
          "propertyOrder" : 1700,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "attributeMapperConfiguration" : {
          "title" : "Attribute Mapper Configuration",
          "description" : "Mapping of OAuth attributes to local OpenAM attributes<br><br>Attribute
 configuration that will be used to map the user info obtained from the OAuth 2.0 Provider to the
 local user data store in the OpenAM.<br/><br/>Example: <code>OAuth2.0_attribute=local_attribute</
code>",
          "propertyOrder" : 1800,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "accountMapperConfiguration" : {
          "title" : "Account Mapper Configuration",
          "description" : "Mapping of OAuth account to local OpenAM account<br><br>Attribute
 configuration that will be used to map the account of the user authenticated in the OAuth 2.0
 Provider to the local data store in the OpenAM. Example: <code>OAuth2.0_attribute=local_attribute</
code>",
          "propertyOrder" : 1600,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "accountMapperClass" : {
          "title" : "Account Mapper",
          "description" : "Name of the class implementing the attribute mapping for the
 account search.<br><br>This class is used by the module to map from the account information
 received from the OAuth Identity Provider into OpenAM.<br/><br/>The class must implement
 the <code>org.forgerock.openam.authentication.modules.common.mapping.AttributeMapper</code>
 interface.<br/>Provided implementations
 are:<ul><li>org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper</
li><li>org.forgerock.openam.authentication.modules.oidc.JwtAttributeMapper (can only be used when
 using the openid scope)</li></ul>String constructor parameters can be provided by appending <code>|</
code> separated values.",
          "propertyOrder" : 1500,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "enableRegistrationService" : {
          "title" : "Use IDM as Registration Service",
```

```
          "description" : "Whether to use IDM as an external Registration Service to complete
 registration for new users.<br><br>IDM is called and passed these parameters:<br/><br/
><ul><li><code>clientToken</code>: Signed, encrypted JWT of the OAuth 2.0 authentication state.</
li><li><code>returnParams</code>: Encoded URL parameters, required to be returned to AM to resume
 authentication after registration in IDM is complete.</li></ul>",
          "propertyOrder" : 1350,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "createAccount" : {
          "title" : "Create account if it does not exist",
          "description" : "If the OAuth2 account does not exist in the local OpenAM data store, an
 account will be created dynamically.<br><br>If this is enabled, the account mapper could create
 the account dynamically if there is no account mapped. Before creating the account, a dialog
 prompting for a password and asking for an activation code can be shown if the parameter \"Prompt
 for password setting and activation code\" is enabled.<br /><br />If this flag is not enabled, 3
 alternative options exist:<br/><br/><ol><li>The accounts need to have a user profile in the OpenAM
 User Data Store</li><li>The user does not have a user profile and the \"Ignore Profile\" is set in
 the Authentication Service of the realm.</li><li>The account is mapped to an anonymous account (see
 parameter \"Map to anonymous user\" and \"Anonymous User\")</li></ol>",
          "propertyOrder" : 1360,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "saveAttributesInSession" : {
          "title" : "Save attributes in the session",
          "description" : "If this option is enabled, the attributes configured in the attribute
 mapper will be saved into the OpenAM session",
          "propertyOrder" : 2400,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        }
      }
    }
  }
}
```


Global Operations

Resource path: `/global-config/authentication/modules/authSocialTwitter`

Resource version: `1.0`

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action SocialAuthTwitterModule --global --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action SocialAuthTwitterModule --global --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action SocialAuthTwitterModule --global --actionName nextdescendents
```

read

Usage:

```
am> read SocialAuthTwitterModule --global
```

update

Usage:

```
am> update SocialAuthTwitterModule --global --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "defaults" : {
      "properties" : {
        "accountProvisioning" : {
          "type" : "object",
          "title" : "Account Provisioning",
          "propertyOrder" : 1,
          "properties" : {
            "accountMapperClass" : {
              "title" : "Account Mapper",
              "description" : "Name of the class implementing the attribute mapping for the
 account search.<br><br>This class is used by the module to map from the account information
 received from the OAuth Identity Provider into OpenAM.<br/><br/>The class must implement
 the <code>org.forgerock.openam.authentication.modules.common.mapping.AttributeMapper</code>
 interface.<br/>Provided implementations
 are:<ul><li>org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper</
li><li>org.forgerock.openam.authentication.modules.oidc.JwtAttributeMapper (can only be used when
```

```
 using the openid scope)</li></ul>String constructor parameters can be provided by appending <code>|</
code> separated values.",
              "propertyOrder" : 1500,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            },
            "enableRegistrationService" : {
              "title" : "Use IDM as Registration Service",
              "description" : "Whether to use IDM as an external Registration Service to
 complete registration for new users.<br><br>IDM is called and passed these parameters:<br/><br/
><ul><li><code>clientToken</code>: Signed, encrypted JWT of the OAuth 2.0 authentication state.</
li><li><code>returnParams</code>: Encoded URL parameters, required to be returned to AM to resume
 authentication after registration in IDM is complete.</li></ul>",
              "propertyOrder" : 1350,
              "required" : true,
              "type" : "boolean",
              "exampleValue" : ""
            },
            "accountProviderClass" : {
              "title" : "Account Provider",
              "description" : "Name of the class implementing the account provider.<br><br>This
 class is used by the module to find the account from the attributes mapped by the Account
 Mapper <code>org.forgerock.openam.authentication.modules.common.mapping.AccountProvider</code>
 interface.<br/>String constructor parameters can be provided by appending <code>|</code> separated
 values.",
              "propertyOrder" : 1400,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            },
            "createAccount" : {
              "title" : "Create account if it does not exist",
              "description" : "If the OAuth2 account does not exist in the local OpenAM data store,
 an account will be created dynamically.<br><br>If this is enabled, the account mapper could create
 the account dynamically if there is no account mapped. Before creating the account, a dialog
 prompting for a password and asking for an activation code can be shown if the parameter \"Prompt
 for password setting and activation code\" is enabled.<br /><br />If this flag is not enabled, 3
 alternative options exist:<br/><br/><ol><li>The accounts need to have a user profile in the OpenAM
 User Data Store</li><li>The user does not have a user profile and the \"Ignore Profile\" is set in
 the Authentication Service of the realm.</li><li>The account is mapped to an anonymous account (see
 parameter \"Map to anonymous user\" and \"Anonymous User\")</li></ol>",
              "propertyOrder" : 1360,
              "required" : true,
              "type" : "boolean",
              "exampleValue" : ""
            },
            "attributeMappingClasses" : {
              "title" : "Attribute Mapper",
              "description" : "Name of the class that implements the attribute
 mapping<br><br>This class maps the OAuth properties into OpenAM properties. A custom
 attribute mapper can be provided.<br/><br/>A custom attribute mapper must implement the
 <code>org.forgerock.openam.authentication.modules.common.mapping.AttributeMapper</code>
 interface.<br/>Provided implementations
 are:<ul><li>org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper</
li><li>org.forgerock.openam.authentication.modules.oidc.JwtAttributeMapper (can only be used when
 using the openid scope)</li></ul>String constructor parameters can be provided by appending <code>|</
code> separated values.",
              "propertyOrder" : 1700,
```

```
              "required" : true,
              "items" : {
                "type" : "string"
              },
              "type" : "array",
              "exampleValue" : ""
            },
            "anonymousUserName" : {
              "title" : "Anonymous User",
              "description" : "Username of the OpenAM anonymous user<br><br>The username of the user
 that will represent the anonymous user. This user account must already exist in the realm.",
              "propertyOrder" : 2100,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            },
            "accountMapperConfiguration" : {
              "title" : "Account Mapper Configuration",
              "description" : "Mapping of OAuth account to local OpenAM account<br><br>Attribute
 configuration that will be used to map the account of the user authenticated in the OAuth 2.0
 Provider to the local data store in the OpenAM. Example: <code>OAuth2.0_attribute=local_attribute</
code>",
              "propertyOrder" : 1600,
              "required" : true,
              "items" : {
                "type" : "string"
              },
              "type" : "array",
              "exampleValue" : ""
            },
            "attributeMapperConfiguration" : {
              "title" : "Attribute Mapper Configuration",
              "description" : "Mapping of OAuth attributes to local OpenAM attributes<br><br>Attribute
 configuration that will be used to map the user info obtained from the OAuth 2.0 Provider to the
 local user data store in the OpenAM.<br/><br/>Example: <code>OAuth2.0_attribute=local_attribute</
code>",
              "propertyOrder" : 1800,
              "required" : true,
              "items" : {
                "type" : "string"
              },
              "type" : "array",
              "exampleValue" : ""
            },
            "mapToAnonymousUser" : {
              "title" : "Map to anonymous user",
              "description" : "Enabled anonymous user access to OpenAM for OAuth authenticated
 users<br><br>If selected, the authenticated users in the OAuth 2.0 Provider will be mapped to the
 anonymous user configured in the next parameter.<br/>If not selected the users authenticated will be
 mapped by the parameters configured in the account mapper.<br/><br/><i>NB </i>If <i>Create account if
 it does not exist</i> is enabled, that parameter takes precedence.",
              "propertyOrder" : 2000,
              "required" : true,
              "type" : "boolean",
              "exampleValue" : ""
            },
            "saveAttributesInSession" : {
              "title" : "Save attributes in the session",
```

```
              "description" : "If this option is enabled, the attributes configured in the attribute
 mapper will be saved into the OpenAM session",
              "propertyOrder" : 2400,
              "required" : true,
              "type" : "boolean",
              "exampleValue" : ""
            }
          }
        },
        "core" : {
          "type" : "object",
          "title" : "Core",
          "propertyOrder" : 0,
          "properties" : {
            "authorizeEndpoint" : {
              "title" : "Authentication Endpoint URL",
              "description" : "OAuth authentication endpoint URL<br><br>This is the URL endpoint for
 OAuth authentication provided by the OAuth Identity Provider",
              "propertyOrder" : 600,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            },
            "requestTokenEndpoint" : {
              "title" : "Request Token Endpoint URL",
              "description" : "OAuth request token endpoint URL<br><br>This is the URL endpoint for
 OAuth request token provided by the OAuth Identity Provider",
              "propertyOrder" : 600,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            },
            "tokenEndpoint" : {
              "title" : "Access Token Endpoint URL",
              "description" : "OAuth access token endpoint URL<br><br>This is the URL endpoint for
 access token retrieval provided by the OAuth Identity Provider. Refer to the <a href=\"http://
tools.ietf.org/html/rfc6749#section-3.2\" target=\"_blank\">RFC 6749</a>, section 3.2",
              "propertyOrder" : 700,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            },
            "clientId" : {
              "title" : "Client Id",
              "description" : "OAuth client_id parameter<br><br>For more information on the OAuth
 client_id parameter refer to the <a href=\"http://tools.ietf.org/html/rfc6749#section-2.3.1\" target=
\"_blank\">RFC 6749</a>, section 2.3.1",
              "propertyOrder" : 400,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            },
            "ssoProxyUrl" : {
              "title" : "Proxy URL",
              "description" : "The URL to the OpenAM OAuth proxy JSP<br><br>This URL should only be
 changed from the default, if an external server is performing the GET to POST proxying. The default
 is <code>/openam/oauth2c/OAuthProxy.jsp</code>",
              "propertyOrder" : 1300,
              "required" : true,
```

```
              "type" : "string",
              "exampleValue" : ""
            },
            "userInfoEndpoint" : {
              "title" : "User Profile Service URL",
              "description" : "User profile information URL<br><br>This URL endpoint provides user
profile information and is provided by the OAuth Identity Provider<br/><br/><i>NB </i>This URL should
return JSON objects in response",
              "propertyOrder" : 800,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            },
            "usesBasicAuth" : {
              "title" : "Use Basic Auth",
              "description" : "When enabled, the client will use basic auth for authenticating with
the social auth provider. Enabled by default.",
              "propertyOrder" : 1200,
              "required" : true,
              "type" : "boolean",
              "exampleValue" : ""
            },
            "subjectProperty" : {
              "title" : "Subject Property",
              "description" : "Property used to identify which attribute an auth server identifies a
user by.",
              "propertyOrder" : 1100,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            },
            "authenticationLevel" : {
              "title" : "Authentication Level",
              "description" : "The authentication level associated with this module.<br><br>Each
authentication module has an authentication level that can be used to indicate the level of security
associated with the module; 0 is the lowest (and the default).",
              "propertyOrder" : 100,
              "required" : true,
              "type" : "integer",
              "exampleValue" : ""
            },
            "provider" : {
              "title" : "Social Provider",
              "description" : "Social Provider for which this module is being setup.",
              "propertyOrder" : 200,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            },
            "clientSecret" : {
              "title" : "Client Secret",
              "description" : "OAuth client_secret parameter<br><br>For more information on the OAuth
client_secret parameter refer to the <a href=\"http://tools.ietf.org/html/rfc6749#section-2.3.1\"
target=\"_blank\">RFC 6749</a>, section 2.3.1",
              "propertyOrder" : 500,
              "required" : true,
              "type" : "string",
              "format" : "password",
              "exampleValue" : ""
```

```
            }
          }
        }
      },
      "type" : "object",
      "title" : "Realm Defaults"
    }
  }
}
```

SocialAuthVKontakteModule

Realm Operations

Resource path: `/realm-config/authentication/modules/authSocialVk`

Resource version: `1.0`

create

Usage:

```
am> create SocialAuthVKontakteModule --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "core" : {
      "type" : "object",
      "title" : "Core",
      "propertyOrder" : 0,
      "properties" : {
        "scope" : {
          "title" : "Scope",
          "description" : "OAuth scope; list of user profile properties<br><br>According to the OAuth
 2.0 Authorization Framework, scope is a space-separated list of user profile attributes that the
 client application requires. The list depends on the permissions that the resource owner grants to
 the client application.<br/><br/> Some authorization servers use non-standard separators for scopes.
 For example, Facebook takes a comma-separated list.<br/><br/>",
          "propertyOrder" : 800,
          "required" : true,
```

```
          "items" : {
            "type" : "string"
          },
          "minItems" : 1,
          "type" : "array",
          "exampleValue" : ""
        },
        "clientSecret" : {
          "title" : "Client Secret",
          "description" : "OAuth client_secret parameter<br><br>For more information on the OAuth
client_secret parameter refer to the <a href=\"http://tools.ietf.org/html/rfc6749#section-2.3.1\"
target=\"_blank\">RFC 6749</a>, section 2.3.1",
          "propertyOrder" : 300,
          "required" : true,
          "type" : "string",
          "format" : "password",
          "exampleValue" : ""
        },
        "ssoProxyUrl" : {
          "title" : "Proxy URL",
          "description" : "The URL to the OpenAM OAuth proxy JSP<br><br>This URL should only be
changed from the default, if an external server is performing the GET to POST proxying. The default
is <code>/openam/oauth2c/OAuthProxy.jsp</code>",
          "propertyOrder" : 900,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "provider" : {
          "title" : "Social Provider",
          "description" : "Social Provider for which this module is being setup.",
          "propertyOrder" : 100,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "forgerock-am-auth-socialauthvk-auth-level" : {
          "title" : "Authentication Level",
          "description" : "The authentication level associated with this module.<br><br>Each
authentication module has an authentication level that can be used to indicate the level of security
associated with the module; 0 is the lowest (and the default).",
          "propertyOrder" : 400,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "authorizeEndpoint" : {
          "title" : "Authentication Endpoint URL",
          "description" : "OAuth authentication endpoint URL<br><br>This is the URL endpoint for OAuth
authentication provided by the OAuth Identity Provider",
          "propertyOrder" : 500,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "tokenEndpoint" : {
          "title" : "Access Token Endpoint URL",
```

```
          "description" : "OAuth access token endpoint URL<br><br>This is the URL endpoint for
 access token retrieval provided by the OAuth Identity Provider. Refer to the <a href=\"http://
tools.ietf.org/html/rfc6749#section-3.2\" target=\"_blank\">RFC 6749</a>, section 3.2",
          "propertyOrder" : 600,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "apiVersion" : {
          "title" : "API Version",
          "description" : "Specifies the version of the auth server API",
          "propertyOrder" : 2100,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "subjectProperty" : {
          "title" : "Subject Property",
          "description" : "Property used to identify which attribute an auth server identifies a user
 by.",
          "propertyOrder" : 1000,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "userInfoEndpoint" : {
          "title" : "User Profile Service URL",
          "description" : "User profile information URL<br><br>This URL endpoint provides user profile
 information and is provided by the OAuth Identity Provider<br/><br/><i>NB </i>This URL should return
 JSON objects in response",
          "propertyOrder" : 700,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "clientId" : {
          "title" : "Client Id",
          "description" : "OAuth client_id parameter<br><br>For more information on the OAuth
 client_id parameter refer to the <a href=\"http://tools.ietf.org/html/rfc6749#section-2.3.1\" target=
\"_blank\">RFC 6749</a>, section 2.3.1",
          "propertyOrder" : 200,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "accountProvisioning" : {
      "type" : "object",
      "title" : "Account Provisioning",
      "propertyOrder" : 1,
      "properties" : {
        "enableRegistrationService" : {
          "title" : "Use IDM as Registration Service",
          "description" : "Whether to use IDM as an external Registration Service to complete
 registration for new users.<br><br>IDM is called and passed these parameters:<br/><br/
><ul><li><code>clientToken</code>: Signed, encrypted JWT of the OAuth 2.0 authentication state.</
li><li><code>returnParams</code>: Encoded URL parameters, required to be returned to AM to resume
 authentication after registration in IDM is complete.</li></ul>",
```

```
          "propertyOrder" : 1150,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "attributeMappingClasses" : {
          "title" : "Attribute Mapper",
          "description" : "Name of the class that implements the attribute
 mapping<br><br>This class maps the OAuth properties into OpenAM properties. A custom
 attribute mapper can be provided.<br/><br/>A custom attribute mapper must implement the
 <code>org.forgerock.openam.authentication.modules.common.mapping.AttributeMapper</code>
 interface.<br/>Provided implementations
 are:<ul><li>org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper</
li><li>org.forgerock.openam.authentication.modules.oidc.JwtAttributeMapper (can only be used when
 using the openid scope)</li></ul>String constructor parameters can be provided by appending <code>|</
code> separated values.",
          "propertyOrder" : 1400,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "anonymousUserName" : {
          "title" : "Anonymous User",
          "description" : "Username of the OpenAM anonymous user<br><br>The username of the user that
 will represent the anonymous user. This user account must already exist in the realm.",
          "propertyOrder" : 1800,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "attributeMapperConfiguration" : {
          "title" : "Attribute Mapper Configuration",
          "description" : "Mapping of OAuth attributes to local OpenAM attributes<br><br>Attribute
 configuration that will be used to map the user info obtained from the OAuth 2.0 Provider to the
 local user data store in the OpenAM.<br/><br/>Example: <code>OAuth2.0_attribute=local_attribute</
code>",
          "propertyOrder" : 1500,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "accountMapperClass" : {
          "title" : "Account Mapper",
          "description" : "Name of the class implementing the attribute mapping for the
 account search.<br><br>This class is used by the module to map from the account information
 received from the OAuth Identity Provider into OpenAM.<br/><br/>The class must implement
 the <code>org.forgerock.openam.authentication.modules.common.mapping.AttributeMapper</code>
 interface.<br/>Provided implementations
 are:<ul><li>org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper</
li><li>org.forgerock.openam.authentication.modules.oidc.JwtAttributeMapper (can only be used when
 using the openid scope)</li></ul>String constructor parameters can be provided by appending <code>|</
code> separated values.",
          "propertyOrder" : 1200,
```

```
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "saveAttributesInSession" : {
          "title" : "Save attributes in the session",
          "description" : "If this option is enabled, the attributes configured in the attribute
 mapper will be saved into the OpenAM session",
          "propertyOrder" : 2000,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "accountProviderClass" : {
          "title" : "Account Provider",
          "description" : "Name of the class implementing the account provider.<br><br>This
 class is used by the module to find the account from the attributes mapped by the Account
 Mapper <code>org.forgerock.openam.authentication.modules.common.mapping.AccountProvider</code>
 interface.<br/>String constructor parameters can be provided by appending <code>|</code> separated
 values.",
          "propertyOrder" : 1100,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "promptPasswordFlag" : {
          "title" : "Prompt for password setting and activation code",
          "description" : "Users must set a password and complete the activation flow during dynamic
 profile creation.<br><br>If this is enabled, the user must set a password before the system creates
 an account dynamically and an activation code will be sent to the user's email address. The account
 will be created only if the password and activation code are properly set. <br />If this is disabled,
 the account will be created transparently without prompting the user.",
          "propertyOrder" : 1605,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "accountMapperConfiguration" : {
          "title" : "Account Mapper Configuration",
          "description" : "Mapping of OAuth account to local OpenAM account<br><br>Attribute
 configuration that will be used to map the account of the user authenticated in the OAuth 2.0
 Provider to the local data store in the OpenAM. Example: <code>OAuth2.0_attribute=local_attribute</
code>",
          "propertyOrder" : 1300,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "mapToAnonymousUser" : {
          "title" : "Map to anonymous user",
          "description" : "Enabled anonymous user access to OpenAM for OAuth authenticated
 users<br><br>If selected, the authenticated users in the OAuth 2.0 Provider will be mapped to the
 anonymous user configured in the next parameter.<br/>If not selected the users authenticated will be
 mapped by the parameters configured in the account mapper.<br/><br/><i>NB </i>If <i>Create account if
 it does not exist</i> is enabled, that parameter takes precedence.",
          "propertyOrder" : 1700,
```

```
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "createAccount" : {
          "title" : "Create account if it does not exist",
          "description" : "If the OAuth2 account does not exist in the local OpenAM data store, an
account will be created dynamically.<br><br>If this is enabled, the account mapper could create
the account dynamically if there is no account mapped. Before creating the account, a dialog
prompting for a password and asking for an activation code can be shown if the parameter \"Prompt
for password setting and activation code\" is enabled.<br /><br />If this flag is not enabled, 3
alternative options exist:<br/><br/><ol><li>The accounts need to have a user profile in the OpenAM
User Data Store</li><li>The user does not have a user profile and the \"Ignore Profile\" is set in
the Authentication Service of the realm.</li><li>The account is mapped to an anonymous account (see
parameter \"Map to anonymous user\" and \"Anonymous User\")</li></ol>",
          "propertyOrder" : 1160,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        }
      }
    },
    "emailSettings" : {
      "type" : "object",
      "title" : "Email",
      "propertyOrder" : 2,
      "properties" : {
        "emailAttribute" : {
          "title" : "Email attribute in the Response",
          "description" : "Attribute from the response used to send activation code emails.<br><br>The
attribute in the response from the profile service of the Provider that contains the email address of
the authenticated user. This address will be used to send an email with an activation code when the
accounts are allowed to be created dynamically.",
          "propertyOrder" : 1610,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "smtpSslEnabled" : {
          "title" : "SMTP SSL Enabled",
          "description" : "Tick this option if the SMTP Server provides SSL",
          "propertyOrder" : 1640,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "smtpFromAddress" : {
          "title" : "SMTP From address",
          "description" : "The email address on behalf of whom the messages will be sent",
          "propertyOrder" : 1645,
          "required" : true,
          "type" : "string",
          "exampleValue" : "info@forgerock.com"
        },
        "smtpPassword" : {
          "title" : "SMTP User Password",
          "description" : "The Password of the SMTP User Name",
          "propertyOrder" : 1635,
          "required" : true,
```

```
          "type" : "string",
          "format" : "password",
          "exampleValue" : ""
        },
        "emailGateway" : {
          "title" : "Mail Server Gateway implementation class",
          "description" : "The class used by the module to send email.<br><br>This class is used by
 the module to send email. A custom implementation can be provided.<br/><br/>The custom implementation
 must implement the <code>org.forgerock.openam.authentication.modules.oauth2.EmailGateway</code>",
          "propertyOrder" : 1615,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "smtpPort" : {
          "title" : "SMTP port",
          "description" : "The TCP port that will be used by the SMTP gateway",
          "propertyOrder" : 1625,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "smtpUsername" : {
          "title" : "SMTP User Name",
          "description" : "If the SMTP Service requires authentication, configure the user name here",
          "propertyOrder" : 1630,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "smtpHost" : {
          "title" : "SMTP host",
          "description" : "The mail host that will be used by the Email Gateway implementation",
          "propertyOrder" : 1620,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    }
  }
}
```

delete

Usage:

```
am> delete SocialAuthVKontakteModule --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action SocialAuthVKontakteModule --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action SocialAuthVKontakteModule --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action SocialAuthVKontakteModule --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query SocialAuthVKontakteModule --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read SocialAuthVKontakteModule --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update SocialAuthVKontakteModule --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "core" : {
      "type" : "object",
      "title" : "Core",
      "propertyOrder" : 0,
      "properties" : {
        "scope" : {
          "title" : "Scope",
          "description" : "OAuth scope; list of user profile properties<br><br>According to the OAuth
 2.0 Authorization Framework, scope is a space-separated list of user profile attributes that the
 client application requires. The list depends on the permissions that the resource owner grants to
 the client application.<br/><br/> Some authorization servers use non-standard separators for scopes.
 For example, Facebook takes a comma-separated list.<br/><br/>",
          "propertyOrder" : 800,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "minItems" : 1,
          "type" : "array",
          "exampleValue" : ""
        },
        "clientSecret" : {
          "title" : "Client Secret",
          "description" : "OAuth client_secret parameter<br><br>For more information on the OAuth
 client_secret parameter refer to the <a href=\"http://tools.ietf.org/html/rfc6749#section-2.3.1\"
 target=\"_blank\">RFC 6749</a>, section 2.3.1",
          "propertyOrder" : 300,
          "required" : true,
          "type" : "string",
          "format" : "password",
          "exampleValue" : ""
        },
        "ssoProxyUrl" : {
          "title" : "Proxy URL",
          "description" : "The URL to the OpenAM OAuth proxy JSP<br><br>This URL should only be
 changed from the default, if an external server is performing the GET to POST proxying. The default
 is <code>/openam/oauth2c/OAuthProxy.jsp</code>",
          "propertyOrder" : 900,
          "required" : true,
```

```
          "type" : "string",
          "exampleValue" : ""
        },
        "provider" : {
          "title" : "Social Provider",
          "description" : "Social Provider for which this module is being setup.",
          "propertyOrder" : 100,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "forgerock-am-auth-socialauthvk-auth-level" : {
          "title" : "Authentication Level",
          "description" : "The authentication level associated with this module.<br><br>Each
 authentication module has an authentication level that can be used to indicate the level of security
 associated with the module; 0 is the lowest (and the default).",
          "propertyOrder" : 400,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "authorizeEndpoint" : {
          "title" : "Authentication Endpoint URL",
          "description" : "OAuth authentication endpoint URL<br><br>This is the URL endpoint for OAuth
 authentication provided by the OAuth Identity Provider",
          "propertyOrder" : 500,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "tokenEndpoint" : {
          "title" : "Access Token Endpoint URL",
          "description" : "OAuth access token endpoint URL<br><br>This is the URL endpoint for
 access token retrieval provided by the OAuth Identity Provider. Refer to the <a href=\"http://
tools.ietf.org/html/rfc6749#section-3.2\" target=\"_blank\">RFC 6749</a>, section 3.2",
          "propertyOrder" : 600,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "apiVersion" : {
          "title" : "API Version",
          "description" : "Specifies the version of the auth server API",
          "propertyOrder" : 2100,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "subjectProperty" : {
          "title" : "Subject Property",
          "description" : "Property used to identify which attribute an auth server identifies a user
 by.",
          "propertyOrder" : 1000,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "userInfoEndpoint" : {
          "title" : "User Profile Service URL",
```

```
          "description" : "User profile information URL<br><br>This URL endpoint provides user profile
 information and is provided by the OAuth Identity Provider<br/><br/><i>NB </i>This URL should return
 JSON objects in response",
          "propertyOrder" : 700,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "clientId" : {
          "title" : "Client Id",
          "description" : "OAuth client_id parameter<br><br>For more information on the OAuth
 client_id parameter refer to the <a href=\"http://tools.ietf.org/html/rfc6749#section-2.3.1\" target=
\"_blank\">RFC 6749</a>, section 2.3.1",
          "propertyOrder" : 200,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "accountProvisioning" : {
      "type" : "object",
      "title" : "Account Provisioning",
      "propertyOrder" : 1,
      "properties" : {
        "enableRegistrationService" : {
          "title" : "Use IDM as Registration Service",
          "description" : "Whether to use IDM as an external Registration Service to complete
 registration for new users.<br><br>IDM is called and passed these parameters:<br/><br/
><ul><li><code>clientToken</code>: Signed, encrypted JWT of the OAuth 2.0 authentication state.</
li><li><code>returnParams</code>: Encoded URL parameters, required to be returned to AM to resume
 authentication after registration in IDM is complete.</li></ul>",
          "propertyOrder" : 1150,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "attributeMappingClasses" : {
          "title" : "Attribute Mapper",
          "description" : "Name of the class that implements the attribute
 mapping<br><br>This class maps the OAuth properties into OpenAM properties. A custom
 attribute mapper can be provided.<br/><br/>A custom attribute mapper must implement the
 <code>org.forgerock.openam.authentication.modules.common.mapping.AttributeMapper</code>
 interface.<br/>Provided implementations
 are:<ul><li>org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper</
li><li>org.forgerock.openam.authentication.modules.oidc.JwtAttributeMapper (can only be used when
 using the openid scope)</li></ul>String constructor parameters can be provided by appending <code>|</
code> separated values.",
          "propertyOrder" : 1400,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "anonymousUserName" : {
          "title" : "Anonymous User",
```

```
          "description" : "Username of the OpenAM anonymous user<br><br>The username of the user that
 will represent the anonymous user. This user account must already exist in the realm.",
          "propertyOrder" : 1800,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "attributeMapperConfiguration" : {
          "title" : "Attribute Mapper Configuration",
          "description" : "Mapping of OAuth attributes to local OpenAM attributes<br><br>Attribute
 configuration that will be used to map the user info obtained from the OAuth 2.0 Provider to the
 local user data store in the OpenAM.<br/><br/>Example: <code>OAuth2.0_attribute=local_attribute</
code>",
          "propertyOrder" : 1500,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "accountMapperClass" : {
          "title" : "Account Mapper",
          "description" : "Name of the class implementing the attribute mapping for the
 account search.<br><br>This class is used by the module to map from the account information
 received from the OAuth Identity Provider into OpenAM.<br/><br/>The class must implement
 the <code>org.forgerock.openam.authentication.modules.common.mapping.AttributeMapper</code>
 interface.<br/>Provided implementations
 are:<ul><li>org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper</
li><li>org.forgerock.openam.authentication.modules.oidc.JwtAttributeMapper (can only be used when
 using the openid scope)</li></ul>String constructor parameters can be provided by appending <code>|</
code> separated values.",
          "propertyOrder" : 1200,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "saveAttributesInSession" : {
          "title" : "Save attributes in the session",
          "description" : "If this option is enabled, the attributes configured in the attribute
 mapper will be saved into the OpenAM session",
          "propertyOrder" : 2000,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "accountProviderClass" : {
          "title" : "Account Provider",
          "description" : "Name of the class implementing the account provider.<br><br>This
 class is used by the module to find the account from the attributes mapped by the Account
 Mapper <code>org.forgerock.openam.authentication.modules.common.mapping.AccountProvider</code>
 interface.<br/>String constructor parameters can be provided by appending <code>|</code> separated
 values.",
          "propertyOrder" : 1100,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "promptPasswordFlag" : {
```

```
          "title" : "Prompt for password setting and activation code",
          "description" : "Users must set a password and complete the activation flow during dynamic
 profile creation.<br><br>If this is enabled, the user must set a password before the system creates
 an account dynamically and an activation code will be sent to the user's email address. The account
 will be created only if the password and activation code are properly set. <br />If this is disabled,
 the account will be created transparently without prompting the user.",
          "propertyOrder" : 1605,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "accountMapperConfiguration" : {
          "title" : "Account Mapper Configuration",
          "description" : "Mapping of OAuth account to local OpenAM account<br><br>Attribute
 configuration that will be used to map the account of the user authenticated in the OAuth 2.0
 Provider to the local data store in the OpenAM. Example: <code>OAuth2.0_attribute=local_attribute</
code>",
          "propertyOrder" : 1300,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "mapToAnonymousUser" : {
          "title" : "Map to anonymous user",
          "description" : "Enabled anonymous user access to OpenAM for OAuth authenticated
 users<br><br>If selected, the authenticated users in the OAuth 2.0 Provider will be mapped to the
 anonymous user configured in the next parameter.<br/>If not selected the users authenticated will be
 mapped by the parameters configured in the account mapper.<br/><br/><i>NB </i>If <i>Create account if
 it does not exist</i> is enabled, that parameter takes precedence.",
          "propertyOrder" : 1700,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "createAccount" : {
          "title" : "Create account if it does not exist",
          "description" : "If the OAuth2 account does not exist in the local OpenAM data store, an
 account will be created dynamically.<br><br>If this is enabled, the account mapper could create
 the account dynamically if there is no account mapped. Before creating the account, a dialog
 prompting for a password and asking for an activation code can be shown if the parameter \"Prompt
 for password setting and activation code\" is enabled.<br /><br />If this flag is not enabled, 3
 alternative options exist:<br/><br/><ol><li>The accounts need to have a user profile in the OpenAM
 User Data Store</li><li>The user does not have a user profile and the \"Ignore Profile\" is set in
 the Authentication Service of the realm.</li><li>The account is mapped to an anonymous account (see
 parameter \"Map to anonymous user\" and \"Anonymous User\")</li></ol>",
          "propertyOrder" : 1160,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        }
      }
    },
    "emailSettings" : {
      "type" : "object",
      "title" : "Email",
      "propertyOrder" : 2,
```

```
     "properties" : {
       "emailAttribute" : {
         "title" : "Email attribute in the Response",
         "description" : "Attribute from the response used to send activation code emails.<br><br>The
attribute in the response from the profile service of the Provider that contains the email address of
the authenticated user. This address will be used to send an email with an activation code when the
accounts are allowed to be created dynamically.",
         "propertyOrder" : 1610,
         "required" : true,
         "type" : "string",
         "exampleValue" : ""
       },
       "smtpSslEnabled" : {
         "title" : "SMTP SSL Enabled",
         "description" : "Tick this option if the SMTP Server provides SSL",
         "propertyOrder" : 1640,
         "required" : true,
         "type" : "boolean",
         "exampleValue" : ""
       },
       "smtpFromAddress" : {
         "title" : "SMTP From address",
         "description" : "The email address on behalf of whom the messages will be sent",
         "propertyOrder" : 1645,
         "required" : true,
         "type" : "string",
         "exampleValue" : "info@forgerock.com"
       },
       "smtpPassword" : {
         "title" : "SMTP User Password",
         "description" : "The Password of the SMTP User Name",
         "propertyOrder" : 1635,
         "required" : true,
         "type" : "string",
         "format" : "password",
         "exampleValue" : ""
       },
       "emailGateway" : {
         "title" : "Mail Server Gateway implementation class",
         "description" : "The class used by the module to send email.<br><br>This class is used by
the module to send email. A custom implementation can be provided.<br/><br/>The custom implementation
must implement the <code>org.forgerock.openam.authentication.modules.oauth2.EmailGateway</code>",
         "propertyOrder" : 1615,
         "required" : true,
         "type" : "string",
         "exampleValue" : ""
       },
       "smtpPort" : {
         "title" : "SMTP port",
         "description" : "The TCP port that will be used by the SMTP gateway",
         "propertyOrder" : 1625,
         "required" : true,
         "type" : "string",
         "exampleValue" : ""
       },
       "smtpUsername" : {
         "title" : "SMTP User Name",
         "description" : "If the SMTP Service requires authentication, configure the user name here",
         "propertyOrder" : 1630,
```

```
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "smtpHost" : {
          "title" : "SMTP host",
          "description" : "The mail host that will be used by the Email Gateway implementation",
          "propertyOrder" : 1620,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    }
  }
}
```

Global Operations

Resource path: `/global-config/authentication/modules/authSocialVk`

Resource version: `1.0`

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action SocialAuthVKontakteModule --global --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action SocialAuthVKontakteModule --global --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action SocialAuthVKontakteModule --global --actionName nextdescendents
```

read

Usage:

```
am> read SocialAuthVKontakteModule --global
```

update

Usage:

```
am> update SocialAuthVKontakteModule --global --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "defaults" : {
      "properties" : {
        "emailSettings" : {
          "type" : "object",
          "title" : "Email",
          "propertyOrder" : 2,
          "properties" : {
            "smtpPort" : {
              "title" : "SMTP port",
              "description" : "The TCP port that will be used by the SMTP gateway",
              "propertyOrder" : 1625,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            },
            "emailAttribute" : {
              "title" : "Email attribute in the Response",
              "description" : "Attribute from the response used to send activation code
emails.<br><br>The attribute in the response from the profile service of the Provider that contains
the email address of the authenticated user. This address will be used to send an email with an
activation code when the accounts are allowed to be created dynamically.",
              "propertyOrder" : 1610,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            },
            "smtpPassword" : {
              "title" : "SMTP User Password",
              "description" : "The Password of the SMTP User Name",
              "propertyOrder" : 1635,
              "required" : true,
              "type" : "string",
              "format" : "password",
              "exampleValue" : ""
            },
            "smtpSslEnabled" : {
              "title" : "SMTP SSL Enabled",
              "description" : "Tick this option if the SMTP Server provides SSL",
```

```
              "propertyOrder" : 1640,
              "required" : true,
              "type" : "boolean",
              "exampleValue" : ""
            },
            "smtpUsername" : {
              "title" : "SMTP User Name",
              "description" : "If the SMTP Service requires authentication, configure the user name
here",
              "propertyOrder" : 1630,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            },
            "smtpHost" : {
              "title" : "SMTP host",
              "description" : "The mail host that will be used by the Email Gateway implementation",
              "propertyOrder" : 1620,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            },
            "smtpFromAddress" : {
              "title" : "SMTP From address",
              "description" : "The email address on behalf of whom the messages will be sent",
              "propertyOrder" : 1645,
              "required" : true,
              "type" : "string",
              "exampleValue" : "info@forgerock.com"
            },
            "emailGateway" : {
              "title" : "Mail Server Gateway implementation class",
              "description" : "The class used by the module to send
email.<br><br>This class is used by the module to send email. A custom
implementation can be provided.<br/><br/>The custom implementation must implement the
<code>org.forgerock.openam.authentication.modules.oauth2.EmailGateway</code>",
              "propertyOrder" : 1615,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            }
          }
        },
        "core" : {
          "type" : "object",
          "title" : "Core",
          "propertyOrder" : 0,
          "properties" : {
            "ssoProxyUrl" : {
              "title" : "Proxy URL",
              "description" : "The URL to the OpenAM OAuth proxy JSP<br><br>This URL should only be
changed from the default, if an external server is performing the GET to POST proxying. The default
is <code>/openam/oauth2c/OAuthProxy.jsp</code>",
              "propertyOrder" : 900,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            },
            "clientId" : {
```

```
              "title" : "Client Id",
              "description" : "OAuth client_id parameter<br><br>For more information on the OAuth
 client_id parameter refer to the <a href=\"http://tools.ietf.org/html/rfc6749#section-2.3.1\" target=
\"_blank\">RFC 6749</a>, section 2.3.1",
              "propertyOrder" : 200,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            },
            "provider" : {
              "title" : "Social Provider",
              "description" : "Social Provider for which this module is being setup.",
              "propertyOrder" : 100,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            },
            "apiVersion" : {
              "title" : "API Version",
              "description" : "Specifies the version of the auth server API",
              "propertyOrder" : 2100,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            },
            "subjectProperty" : {
              "title" : "Subject Property",
              "description" : "Property used to identify which attribute an auth server identifies a
 user by.",
              "propertyOrder" : 1000,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            },
            "tokenEndpoint" : {
              "title" : "Access Token Endpoint URL",
              "description" : "OAuth access token endpoint URL<br><br>This is the URL endpoint for
 access token retrieval provided by the OAuth Identity Provider. Refer to the <a href=\"http://
tools.ietf.org/html/rfc6749#section-3.2\" target=\"_blank\">RFC 6749</a>, section 3.2",
              "propertyOrder" : 600,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            },
            "clientSecret" : {
              "title" : "Client Secret",
              "description" : "OAuth client_secret parameter<br><br>For more information on the OAuth
 client_secret parameter refer to the <a href=\"http://tools.ietf.org/html/rfc6749#section-2.3.1\"
 target=\"_blank\">RFC 6749</a>, section 2.3.1",
              "propertyOrder" : 300,
              "required" : true,
              "type" : "string",
              "format" : "password",
              "exampleValue" : ""
            },
            "scope" : {
              "title" : "Scope",
              "description" : "OAuth scope; list of user profile properties<br><br>According to the
 OAuth 2.0 Authorization Framework, scope is a space-separated list of user profile attributes that
```

```
 the client application requires. The list depends on the permissions that the resource owner grants
 to the client application.<br/><br/> Some authorization servers use non-standard separators for
 scopes. For example, Facebook takes a comma-separated list.<br/><br/>",
              "propertyOrder" : 800,
              "required" : true,
              "items" : {
                "type" : "string"
              },
              "type" : "array",
              "exampleValue" : ""
            },
            "forgerock-am-auth-socialauthvk-auth-level" : {
              "title" : "Authentication Level",
              "description" : "The authentication level associated with this module.<br><br>Each
 authentication module has an authentication level that can be used to indicate the level of security
 associated with the module; 0 is the lowest (and the default).",
              "propertyOrder" : 400,
              "required" : true,
              "type" : "integer",
              "exampleValue" : ""
            },
            "userInfoEndpoint" : {
              "title" : "User Profile Service URL",
              "description" : "User profile information URL<br><br>This URL endpoint provides user
 profile information and is provided by the OAuth Identity Provider<br/><br/><i>NB </i>This URL should
 return JSON objects in response",
              "propertyOrder" : 700,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            },
            "authorizeEndpoint" : {
              "title" : "Authentication Endpoint URL",
              "description" : "OAuth authentication endpoint URL<br><br>This is the URL endpoint for
 OAuth authentication provided by the OAuth Identity Provider",
              "propertyOrder" : 500,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            }
          }
        },
        "accountProvisioning" : {
          "type" : "object",
          "title" : "Account Provisioning",
          "propertyOrder" : 1,
          "properties" : {
            "attributeMappingClasses" : {
              "title" : "Attribute Mapper",
              "description" : "Name of the class that implements the attribute
 mapping<br><br>This class maps the OAuth properties into OpenAM properties. A custom
 attribute mapper can be provided.<br/><br/>A custom attribute mapper must implement the
 <code>org.forgerock.openam.authentication.modules.common.mapping.AttributeMapper</code>
 interface.<br/>Provided implementations
 are:<ul><li>org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper</
li><li>org.forgerock.openam.authentication.modules.oidc.JwtAttributeMapper (can only be used when
 using the openid scope)</li></ul>String constructor parameters can be provided by appending <code>|</
code> separated values.",
              "propertyOrder" : 1400,
```

```
              "required" : true,
              "items" : {
                "type" : "string"
              },
              "type" : "array",
              "exampleValue" : ""
            },
            "accountMapperConfiguration" : {
              "title" : "Account Mapper Configuration",
              "description" : "Mapping of OAuth account to local OpenAM account<br><br>Attribute
 configuration that will be used to map the account of the user authenticated in the OAuth 2.0
 Provider to the local data store in the OpenAM. Example: <code>OAuth2.0_attribute=local_attribute</
code>",
              "propertyOrder" : 1300,
              "required" : true,
              "items" : {
                "type" : "string"
              },
              "type" : "array",
              "exampleValue" : ""
            },
            "enableRegistrationService" : {
              "title" : "Use IDM as Registration Service",
              "description" : "Whether to use IDM as an external Registration Service to
 complete registration for new users.<br><br>IDM is called and passed these parameters:<br/><br/
><ul><li><code>clientToken</code>: Signed, encrypted JWT of the OAuth 2.0 authentication state.</
li><li><code>returnParams</code>: Encoded URL parameters, required to be returned to AM to resume
 authentication after registration in IDM is complete.</li></ul>",
              "propertyOrder" : 1150,
              "required" : true,
              "type" : "boolean",
              "exampleValue" : ""
            },
            "anonymousUserName" : {
              "title" : "Anonymous User",
              "description" : "Username of the OpenAM anonymous user<br><br>The username of the user
 that will represent the anonymous user. This user account must already exist in the realm.",
              "propertyOrder" : 1800,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            },
            "attributeMapperConfiguration" : {
              "title" : "Attribute Mapper Configuration",
              "description" : "Mapping of OAuth attributes to local OpenAM attributes<br><br>Attribute
 configuration that will be used to map the user info obtained from the OAuth 2.0 Provider to the
 local user data store in the OpenAM.<br/><br/>Example: <code>OAuth2.0_attribute=local_attribute</
code>",
              "propertyOrder" : 1500,
              "required" : true,
              "items" : {
                "type" : "string"
              },
              "type" : "array",
              "exampleValue" : ""
            },
            "promptPasswordFlag" : {
              "title" : "Prompt for password setting and activation code",
```

```
              "description" : "Users must set a password and complete the activation flow during
 dynamic profile creation.<br><br>If this is enabled, the user must set a password before the system
 creates an account dynamically and an activation code will be sent to the user's email address. The
 account will be created only if the password and activation code are properly set. <br />If this is
 disabled, the account will be created transparently without prompting the user.",
              "propertyOrder" : 1605,
              "required" : true,
              "type" : "boolean",
              "exampleValue" : ""
            },
            "accountMapperClass" : {
              "title" : "Account Mapper",
              "description" : "Name of the class implementing the attribute mapping for the
 account search.<br><br>This class is used by the module to map from the account information
 received from the OAuth Identity Provider into OpenAM.<br/><br/>The class must implement
 the <code>org.forgerock.openam.authentication.modules.common.mapping.AttributeMapper</code>
 interface.<br/>Provided implementations
 are:<ul><li>org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper</
li><li>org.forgerock.openam.authentication.modules.oidc.JwtAttributeMapper (can only be used when
 using the openid scope)</li></ul>String constructor parameters can be provided by appending <code>|</
code> separated values.",
              "propertyOrder" : 1200,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            },
            "mapToAnonymousUser" : {
              "title" : "Map to anonymous user",
              "description" : "Enabled anonymous user access to OpenAM for OAuth authenticated
 users<br><br>If selected, the authenticated users in the OAuth 2.0 Provider will be mapped to the
 anonymous user configured in the next parameter.<br/>If not selected the users authenticated will be
 mapped by the parameters configured in the account mapper.<br/><br/><i>NB </i>If <i>Create account if
 it does not exist</i> is enabled, that parameter takes precedence.",
              "propertyOrder" : 1700,
              "required" : true,
              "type" : "boolean",
              "exampleValue" : ""
            },
            "accountProviderClass" : {
              "title" : "Account Provider",
              "description" : "Name of the class implementing the account provider.<br><br>This
 class is used by the module to find the account from the attributes mapped by the Account
 Mapper <code>org.forgerock.openam.authentication.modules.common.mapping.AccountProvider</code>
 interface.<br/>String constructor parameters can be provided by appending <code>|</code> separated
 values.",
              "propertyOrder" : 1100,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            },
            "createAccount" : {
              "title" : "Create account if it does not exist",
              "description" : "If the OAuth2 account does not exist in the local OpenAM data store,
 an account will be created dynamically.<br><br>If this is enabled, the account mapper could create
 the account dynamically if there is no account mapped. Before creating the account, a dialog
 prompting for a password and asking for an activation code can be shown if the parameter \"Prompt
 for password setting and activation code\" is enabled.<br /><br />If this flag is not enabled, 3
 alternative options exist:<br/><br/><ol><li>The accounts need to have a user profile in the OpenAM
 User Data Store</li><li>The user does not have a user profile and the \"Ignore Profile\" is set in
```

```
 the Authentication Service of the realm.</li><li>The account is mapped to an anonymous account (see
 parameter \"Map to anonymous user\" and \"Anonymous User\")</li></ol>",
              "propertyOrder" : 1160,
              "required" : true,
              "type" : "boolean",
              "exampleValue" : ""
            },
            "saveAttributesInSession" : {
              "title" : "Save attributes in the session",
              "description" : "If this option is enabled, the attributes configured in the attribute
 mapper will be saved into the OpenAM session",
              "propertyOrder" : 2000,
              "required" : true,
              "type" : "boolean",
              "exampleValue" : ""
            }
          }
        }
      },
      "type" : "object",
      "title" : "Realm Defaults"
    }
  }
}
```

SocialAuthWeChatMobileModule

Realm Operations

Resource path: `/realm-config/authentication/modules/authSocialWeChatMobile`

Resource version: `1.0`

create

Usage:

```
am> create SocialAuthWeChatMobileModule --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
```

```
 "properties" : {
   "emailSettings" : {
     "type" : "object",
     "title" : "Email",
     "propertyOrder" : 2,
     "properties" : {
       "smtpPort" : {
         "title" : "SMTP port",
         "description" : "The TCP port that will be used by the SMTP gateway",
         "propertyOrder" : 1925,
         "required" : true,
         "type" : "string",
         "exampleValue" : ""
       },
       "emailGateway" : {
         "title" : "Mail Server Gateway implementation class",
         "description" : "The class used by the module to send email.<br><br>This class is used by
the module to send email. A custom implementation can be provided.<br/><br/>The custom implementation
must implement the <code>org.forgerock.openam.authentication.modules.oauth2.EmailGateway</code>",
         "propertyOrder" : 1915,
         "required" : true,
         "type" : "string",
         "exampleValue" : ""
       },
       "smtpFromAddress" : {
         "title" : "SMTP From address",
         "description" : "The email address on behalf of whom the messages will be sent",
         "propertyOrder" : 1945,
         "required" : true,
         "type" : "string",
         "exampleValue" : "info@forgerock.com"
       },
       "smtpPassword" : {
         "title" : "SMTP User Password",
         "description" : "The Password of the SMTP User Name",
         "propertyOrder" : 1935,
         "required" : true,
         "type" : "string",
         "format" : "password",
         "exampleValue" : ""
       },
       "smtpUsername" : {
         "title" : "SMTP User Name",
         "description" : "If the SMTP Service requires authentication, configure the user name here",
         "propertyOrder" : 1930,
         "required" : true,
         "type" : "string",
         "exampleValue" : ""
       },
       "emailAttribute" : {
         "title" : "Email attribute in the Response",
         "description" : "Attribute from the response used to send activation code emails.<br><br>The
attribute in the response from the profile service of the Provider that contains the email address of
the authenticated user. This address will be used to send an email with an activation code when the
accounts are allowed to be created dynamically.",
         "propertyOrder" : 1910,
         "required" : true,
         "type" : "string",
         "exampleValue" : ""
```

```
        },
        "smtpHost" : {
          "title" : "SMTP host",
          "description" : "The mail host that will be used by the Email Gateway implementation",
          "propertyOrder" : 1920,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "smtpSslEnabled" : {
          "title" : "SMTP SSL Enabled",
          "description" : "Tick this option if the SMTP Server provides SSL",
          "propertyOrder" : 1940,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        }
      }
    },
    "accountProvisioning" : {
      "type" : "object",
      "title" : "Account Provisioning",
      "propertyOrder" : 1,
      "properties" : {
        "accountProviderClass" : {
          "title" : "Account Provider",
          "description" : "Name of the class implementing the account provider.<br><br>This
 class is used by the module to find the account from the attributes mapped by the Account
 Mapper <code>org.forgerock.openam.authentication.modules.common.mapping.AccountProvider</code>
 interface.<br/>String constructor parameters can be provided by appending <code>|</code> separated
 values.",
          "propertyOrder" : 1400,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "saveAttributesInSession" : {
          "title" : "Save attributes in the session",
          "description" : "If this option is enabled, the attributes configured in the attribute
 mapper will be saved into the OpenAM session",
          "propertyOrder" : 2400,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "accountMapperClass" : {
          "title" : "Account Mapper",
          "description" : "Name of the class implementing the attribute mapping for the
 account search.<br><br>This class is used by the module to map from the account information
 received from the OAuth Identity Provider into OpenAM.<br/><br/>The class must implement
 the <code>org.forgerock.openam.authentication.modules.common.mapping.AttributeMapper</code>
 interface.<br/>Provided implementations
 are:<ul><li>org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper</
li><li>org.forgerock.openam.authentication.modules.oidc.JwtAttributeMapper (can only be used when
 using the openid scope)</li></ul>String constructor parameters can be provided by appending <code>|</
code> separated values.",
          "propertyOrder" : 1500,
          "required" : true,
          "type" : "string",
```

```
          "exampleValue" : ""
        },
        "attributeMappingClasses" : {
          "title" : "Attribute Mapper",
          "description" : "Name of the class that implements the attribute
 mapping<br><br>This class maps the OAuth properties into OpenAM properties. A custom
 attribute mapper can be provided.<br/><br/>A custom attribute mapper must implement the
 <code>org.forgerock.openam.authentication.modules.common.mapping.AttributeMapper</code>
 interface.<br/>Provided implementations
 are:<ul><li>org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper</
li><li>org.forgerock.openam.authentication.modules.oidc.JwtAttributeMapper (can only be used when
 using the openid scope)</li></ul>String constructor parameters can be provided by appending <code>|</
code> separated values.",
          "propertyOrder" : 1700,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "accountMapperConfiguration" : {
          "title" : "Account Mapper Configuration",
          "description" : "Mapping of OAuth account to local OpenAM account<br><br>Attribute
 configuration that will be used to map the account of the user authenticated in the OAuth 2.0
 Provider to the local data store in the OpenAM. Example: <code>OAuth2.0_attribute=local_attribute</
code>",
          "propertyOrder" : 1600,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "enableRegistrationService" : {
          "title" : "Use IDM as Registration Service",
          "description" : "Whether to use IDM as an external Registration Service to complete
 registration for new users.<br><br>IDM is called and passed these parameters:<br/><br/
><ul><li><code>clientToken</code>: Signed, encrypted JWT of the OAuth 2.0 authentication state.</
li><li><code>returnParams</code>: Encoded URL parameters, required to be returned to AM to resume
 authentication after registration in IDM is complete.</li></ul>",
          "propertyOrder" : 1350,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "anonymousUserName" : {
          "title" : "Anonymous User",
          "description" : "Username of the OpenAM anonymous user<br><br>The username of the user that
 will represent the anonymous user. This user account must already exist in the realm.",
          "propertyOrder" : 2100,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "createAccount" : {
          "title" : "Create account if it does not exist",
```

```
          "description" : "If the OAuth2 account does not exist in the local OpenAM data store, an
 account will be created dynamically.<br><br>If this is enabled, the account mapper could create
 the account dynamically if there is no account mapped. Before creating the account, a dialog
 prompting for a password and asking for an activation code can be shown if the parameter \"Prompt
 for password setting and activation code\" is enabled.<br /><br />If this flag is not enabled, 3
 alternative options exist:<br/><br/><ol><li>The accounts need to have a user profile in the OpenAM
 User Data Store</li><li>The user does not have a user profile and the \"Ignore Profile\" is set in
 the Authentication Service of the realm.</li><li>The account is mapped to an anonymous account (see
 parameter \"Map to anonymous user\" and \"Anonymous User\")</li></ol>",
          "propertyOrder" : 1360,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "mapToAnonymousUser" : {
          "title" : "Map to anonymous user",
          "description" : "Enabled anonymous user access to OpenAM for OAuth authenticated
 users<br><br>If selected, the authenticated users in the OAuth 2.0 Provider will be mapped to the
 anonymous user configured in the next parameter.<br/>If not selected the users authenticated will be
 mapped by the parameters configured in the account mapper.<br/><br/><i>NB </i>If <i>Create account if
 it does not exist</i> is enabled, that parameter takes precedence.",
          "propertyOrder" : 2000,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "promptPasswordFlag" : {
          "title" : "Prompt for password setting and activation code",
          "description" : "Users must set a password and complete the activation flow during dynamic
 profile creation.<br><br>If this is enabled, the user must set a password before the system creates
 an account dynamically and an activation code will be sent to the user's email address. The account
 will be created only if the password and activation code are properly set. <br />If this is disabled,
 the account will be created transparently without prompting the user.",
          "propertyOrder" : 1905,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "attributeMapperConfiguration" : {
          "title" : "Attribute Mapper Configuration",
          "description" : "Mapping of OAuth attributes to local OpenAM attributes<br><br>Attribute
 configuration that will be used to map the user info obtained from the OAuth 2.0 Provider to the
 local user data store in the OpenAM.<br/><br/>Example: <code>OAuth2.0_attribute=local_attribute</
code>",
          "propertyOrder" : 1800,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        }
      }
    },
    "core" : {
      "type" : "object",
      "title" : "Core",
      "propertyOrder" : 0,
      "properties" : {
```

```
       "subjectProperty" : {
         "title" : "Subject Property",
         "description" : "Property used to identify which attribute an auth server identifies a user
by.",
         "propertyOrder" : 1100,
         "required" : true,
         "type" : "string",
         "exampleValue" : ""
       },
       "provider" : {
         "title" : "Social Provider",
         "description" : "Social Provider for which this module is being setup.",
         "propertyOrder" : 200,
         "required" : true,
         "type" : "string",
         "exampleValue" : ""
       },
       "ssoProxyUrl" : {
         "title" : "Proxy URL",
         "description" : "The URL to the OpenAM OAuth proxy JSP<br><br>This URL should only be
changed from the default, if an external server is performing the GET to POST proxying. The default
is <code>/openam/oauth2c/OAuthProxy.jsp</code>",
         "propertyOrder" : 1300,
         "required" : true,
         "type" : "string",
         "exampleValue" : ""
       },
       "userInfoEndpoint" : {
         "title" : "User Profile Service URL",
         "description" : "User profile information URL<br><br>This URL endpoint provides user profile
information and is provided by the OAuth Identity Provider<br/><br/><i>NB </i>This URL should return
JSON objects in response",
         "propertyOrder" : 800,
         "required" : true,
         "type" : "string",
         "exampleValue" : ""
       },
       "scope" : {
         "title" : "Scope",
         "description" : "OAuth scope; list of user profile properties<br><br>According to the OAuth
2.0 Authorization Framework, scope is a space-separated list of user profile attributes that the
client application requires. The list depends on the permissions that the resource owner grants to
the client application.<br/><br/> Some authorization servers use non-standard separators for scopes.
For example, Facebook takes a comma-separated list.<br/><br/>",
         "propertyOrder" : 900,
         "required" : true,
         "items" : {
           "type" : "string"
         },
         "minItems" : 1,
         "type" : "array",
         "exampleValue" : ""
       },
       "authenticationLevel" : {
         "title" : "Authentication Level",
         "description" : "The authentication level associated with this module.<br><br>Each
authentication module has an authentication level that can be used to indicate the level of security
associated with the module; 0 is the lowest (and the default).",
         "propertyOrder" : 100,
```

```
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        }
      }
    }
  }
}
```

delete

Usage:

```
am> delete SocialAuthWeChatMobileModule --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action SocialAuthWeChatMobileModule --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action SocialAuthWeChatMobileModule --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action SocialAuthWeChatMobileModule --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query SocialAuthWeChatMobileModule --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read SocialAuthWeChatMobileModule --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update SocialAuthWeChatMobileModule --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "emailSettings" : {
      "type" : "object",
      "title" : "Email",
      "propertyOrder" : 2,
      "properties" : {
        "smtpPort" : {
          "title" : "SMTP port",
          "description" : "The TCP port that will be used by the SMTP gateway",
          "propertyOrder" : 1925,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "emailGateway" : {
```

```
          "title" : "Mail Server Gateway implementation class",
          "description" : "The class used by the module to send email.<br><br>This class is used by
the module to send email. A custom implementation can be provided.<br/><br/>The custom implementation
must implement the <code>org.forgerock.openam.authentication.modules.oauth2.EmailGateway</code>",
          "propertyOrder" : 1915,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "smtpFromAddress" : {
          "title" : "SMTP From address",
          "description" : "The email address on behalf of whom the messages will be sent",
          "propertyOrder" : 1945,
          "required" : true,
          "type" : "string",
          "exampleValue" : "info@forgerock.com"
        },
        "smtpPassword" : {
          "title" : "SMTP User Password",
          "description" : "The Password of the SMTP User Name",
          "propertyOrder" : 1935,
          "required" : true,
          "type" : "string",
          "format" : "password",
          "exampleValue" : ""
        },
        "smtpUsername" : {
          "title" : "SMTP User Name",
          "description" : "If the SMTP Service requires authentication, configure the user name here",
          "propertyOrder" : 1930,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "emailAttribute" : {
          "title" : "Email attribute in the Response",
          "description" : "Attribute from the response used to send activation code emails.<br><br>The
attribute in the response from the profile service of the Provider that contains the email address of
the authenticated user. This address will be used to send an email with an activation code when the
accounts are allowed to be created dynamically.",
          "propertyOrder" : 1910,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "smtpHost" : {
          "title" : "SMTP host",
          "description" : "The mail host that will be used by the Email Gateway implementation",
          "propertyOrder" : 1920,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "smtpSslEnabled" : {
          "title" : "SMTP SSL Enabled",
          "description" : "Tick this option if the SMTP Server provides SSL",
          "propertyOrder" : 1940,
          "required" : true,
          "type" : "boolean",
```

```
          "exampleValue" : ""
        }
      }
    },
    "accountProvisioning" : {
      "type" : "object",
      "title" : "Account Provisioning",
      "propertyOrder" : 1,
      "properties" : {
        "accountProviderClass" : {
          "title" : "Account Provider",
          "description" : "Name of the class implementing the account provider.<br><br>This
 class is used by the module to find the account from the attributes mapped by the Account
 Mapper <code>org.forgerock.openam.authentication.modules.common.mapping.AccountProvider</code>
 interface.<br/>String constructor parameters can be provided by appending <code>|</code> separated
 values.",
          "propertyOrder" : 1400,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "saveAttributesInSession" : {
          "title" : "Save attributes in the session",
          "description" : "If this option is enabled, the attributes configured in the attribute
 mapper will be saved into the OpenAM session",
          "propertyOrder" : 2400,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "accountMapperClass" : {
          "title" : "Account Mapper",
          "description" : "Name of the class implementing the attribute mapping for the
 account search.<br><br>This class is used by the module to map from the account information
 received from the OAuth Identity Provider into OpenAM.<br/><br/>The class must implement
 the <code>org.forgerock.openam.authentication.modules.common.mapping.AttributeMapper</code>
 interface.<br/>Provided implementations
 are:<ul><li>org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper</
li><li>org.forgerock.openam.authentication.modules.oidc.JwtAttributeMapper (can only be used when
 using the openid scope)</li></ul>String constructor parameters can be provided by appending <code>|</
code> separated values.",
          "propertyOrder" : 1500,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "attributeMappingClasses" : {
          "title" : "Attribute Mapper",
          "description" : "Name of the class that implements the attribute
 mapping<br><br>This class maps the OAuth properties into OpenAM properties. A custom
 attribute mapper can be provided.<br/><br/>A custom attribute mapper must implement the
 <code>org.forgerock.openam.authentication.modules.common.mapping.AttributeMapper</code>
 interface.<br/>Provided implementations
 are:<ul><li>org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper</
li><li>org.forgerock.openam.authentication.modules.oidc.JwtAttributeMapper (can only be used when
 using the openid scope)</li></ul>String constructor parameters can be provided by appending <code>|</
code> separated values.",
          "propertyOrder" : 1700,
          "required" : true,
```

```
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "accountMapperConfiguration" : {
          "title" : "Account Mapper Configuration",
          "description" : "Mapping of OAuth account to local OpenAM account<br><br>Attribute
 configuration that will be used to map the account of the user authenticated in the OAuth 2.0
 Provider to the local data store in the OpenAM. Example: <code>OAuth2.0_attribute=local_attribute</
code>",
          "propertyOrder" : 1600,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "enableRegistrationService" : {
          "title" : "Use IDM as Registration Service",
          "description" : "Whether to use IDM as an external Registration Service to complete
 registration for new users.<br><br>IDM is called and passed these parameters:<br/><br/
><ul><li><code>clientToken</code>: Signed, encrypted JWT of the OAuth 2.0 authentication state.</
li><li><code>returnParams</code>: Encoded URL parameters, required to be returned to AM to resume
 authentication after registration in IDM is complete.</li></ul>",
          "propertyOrder" : 1350,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "anonymousUserName" : {
          "title" : "Anonymous User",
          "description" : "Username of the OpenAM anonymous user<br><br>The username of the user that
 will represent the anonymous user. This user account must already exist in the realm.",
          "propertyOrder" : 2100,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "createAccount" : {
          "title" : "Create account if it does not exist",
          "description" : "If the OAuth2 account does not exist in the local OpenAM data store, an
 account will be created dynamically.<br><br>If this is enabled, the account mapper could create
 the account dynamically if there is no account mapped. Before creating the account, a dialog
 prompting for a password and asking for an activation code can be shown if the parameter \"Prompt
 for password setting and activation code\" is enabled.<br /><br />If this flag is not enabled, 3
 alternative options exist:<br/><br/><ol><li>The accounts need to have a user profile in the OpenAM
 User Data Store</li><li>The user does not have a user profile and the \"Ignore Profile\" is set in
 the Authentication Service of the realm.</li><li>The account is mapped to an anonymous account (see
 parameter \"Map to anonymous user\" and \"Anonymous User\")</li></ol>",
          "propertyOrder" : 1360,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "mapToAnonymousUser" : {
          "title" : "Map to anonymous user",
```

```
          "description" : "Enabled anonymous user access to OpenAM for OAuth authenticated
 users<br><br>If selected, the authenticated users in the OAuth 2.0 Provider will be mapped to the
 anonymous user configured in the next parameter.<br/>If not selected the users authenticated will be
 mapped by the parameters configured in the account mapper.<br/><br/><i>NB </i>If <i>Create account if
 it does not exist</i> is enabled, that parameter takes precedence.",
          "propertyOrder" : 2000,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "promptPasswordFlag" : {
          "title" : "Prompt for password setting and activation code",
          "description" : "Users must set a password and complete the activation flow during dynamic
 profile creation.<br><br>If this is enabled, the user must set a password before the system creates
 an account dynamically and an activation code will be sent to the user's email address. The account
 will be created only if the password and activation code are properly set. <br />If this is disabled,
 the account will be created transparently without prompting the user.",
          "propertyOrder" : 1905,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "attributeMapperConfiguration" : {
          "title" : "Attribute Mapper Configuration",
          "description" : "Mapping of OAuth attributes to local OpenAM attributes<br><br>Attribute
 configuration that will be used to map the user info obtained from the OAuth 2.0 Provider to the
 local user data store in the OpenAM.<br/><br/>Example: <code>OAuth2.0_attribute=local_attribute</
code>",
          "propertyOrder" : 1800,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        }
      }
    },
    "core" : {
      "type" : "object",
      "title" : "Core",
      "propertyOrder" : 0,
      "properties" : {
        "subjectProperty" : {
          "title" : "Subject Property",
          "description" : "Property used to identify which attribute an auth server identifies a user
 by.",
          "propertyOrder" : 1100,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "provider" : {
          "title" : "Social Provider",
          "description" : "Social Provider for which this module is being setup.",
          "propertyOrder" : 200,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
```

```
        },
        "ssoProxyUrl" : {
          "title" : "Proxy URL",
          "description" : "The URL to the OpenAM OAuth proxy JSP<br><br>This URL should only be
 changed from the default, if an external server is performing the GET to POST proxying. The default
 is <code>/openam/oauth2c/OAuthProxy.jsp</code>",
          "propertyOrder" : 1300,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "userInfoEndpoint" : {
          "title" : "User Profile Service URL",
          "description" : "User profile information URL<br><br>This URL endpoint provides user profile
 information and is provided by the OAuth Identity Provider<br/><br/><i>NB </i>This URL should return
 JSON objects in response",
          "propertyOrder" : 800,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "scope" : {
          "title" : "Scope",
          "description" : "OAuth scope; list of user profile properties<br><br>According to the OAuth
 2.0 Authorization Framework, scope is a space-separated list of user profile attributes that the
 client application requires. The list depends on the permissions that the resource owner grants to
 the client application.<br/><br/> Some authorization servers use non-standard separators for scopes.
 For example, Facebook takes a comma-separated list.<br/><br/>",
          "propertyOrder" : 900,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "minItems" : 1,
          "type" : "array",
          "exampleValue" : ""
        },
        "authenticationLevel" : {
          "title" : "Authentication Level",
          "description" : "The authentication level associated with this module.<br><br>Each
 authentication module has an authentication level that can be used to indicate the level of security
 associated with the module; 0 is the lowest (and the default).",
          "propertyOrder" : 100,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        }
      }
    }
  }
}
```

Global Operations

Resource path: `/global-config/authentication/modules/authSocialWeChatMobile`

Resource version: `1.0`

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action SocialAuthWeChatMobileModule --global --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action SocialAuthWeChatMobileModule --global --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action SocialAuthWeChatMobileModule --global --actionName nextdescendents
```

read

Usage:

```
am> read SocialAuthWeChatMobileModule --global
```

update

Usage:

```
am> update SocialAuthWeChatMobileModule --global --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "defaults" : {
      "properties" : {
        "accountProvisioning" : {
```

```
          "type" : "object",
          "title" : "Account Provisioning",
          "propertyOrder" : 1,
          "properties" : {
            "promptPasswordFlag" : {
              "title" : "Prompt for password setting and activation code",
              "description" : "Users must set a password and complete the activation flow during
 dynamic profile creation.<br><br>If this is enabled, the user must set a password before the system
 creates an account dynamically and an activation code will be sent to the user's email address. The
 account will be created only if the password and activation code are properly set. <br />If this is
 disabled, the account will be created transparently without prompting the user.",
              "propertyOrder" : 1905,
              "required" : true,
              "type" : "boolean",
              "exampleValue" : ""
            },
            "saveAttributesInSession" : {
              "title" : "Save attributes in the session",
              "description" : "If this option is enabled, the attributes configured in the attribute
 mapper will be saved into the OpenAM session",
              "propertyOrder" : 2400,
              "required" : true,
              "type" : "boolean",
              "exampleValue" : ""
            },
            "attributeMapperConfiguration" : {
              "title" : "Attribute Mapper Configuration",
              "description" : "Mapping of OAuth attributes to local OpenAM attributes<br><br>Attribute
 configuration that will be used to map the user info obtained from the OAuth 2.0 Provider to the
 local user data store in the OpenAM.<br/><br/>Example: <code>OAuth2.0_attribute=local_attribute</
code>",
              "propertyOrder" : 1800,
              "required" : true,
              "items" : {
                "type" : "string"
              },
              "type" : "array",
              "exampleValue" : ""
            },
            "accountMapperClass" : {
              "title" : "Account Mapper",
              "description" : "Name of the class implementing the attribute mapping for the
 account search.<br><br>This class is used by the module to map from the account information
 received from the OAuth Identity Provider into OpenAM.<br/><br/>The class must implement
 the <code>org.forgerock.openam.authentication.modules.common.mapping.AttributeMapper</code>
 interface.<br/>Provided implementations
 are:<ul><li>org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper</
li><li>org.forgerock.openam.authentication.modules.oidc.JwtAttributeMapper (can only be used when
 using the openid scope)</li></ul>String constructor parameters can be provided by appending <code>|</
code> separated values.",
              "propertyOrder" : 1500,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            },
            "accountProviderClass" : {
              "title" : "Account Provider",
              "description" : "Name of the class implementing the account provider.<br><br>This
 class is used by the module to find the account from the attributes mapped by the Account
```

```
 Mapper <code>org.forgerock.openam.authentication.modules.common.mapping.AccountProvider</code>
 interface.<br/>String constructor parameters can be provided by appending <code>|</code> separated
 values.",
              "propertyOrder" : 1400,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            },
            "mapToAnonymousUser" : {
              "title" : "Map to anonymous user",
              "description" : "Enabled anonymous user access to OpenAM for OAuth authenticated
 users<br><br>If selected, the authenticated users in the OAuth 2.0 Provider will be mapped to the
 anonymous user configured in the next parameter.<br/>If not selected the users authenticated will be
 mapped by the parameters configured in the account mapper.<br/><br/><i>NB </i>If <i>Create account if
 it does not exist</i> is enabled, that parameter takes precedence.",
              "propertyOrder" : 2000,
              "required" : true,
              "type" : "boolean",
              "exampleValue" : ""
            },
            "attributeMappingClasses" : {
              "title" : "Attribute Mapper",
              "description" : "Name of the class that implements the attribute
 mapping<br><br>This class maps the OAuth properties into OpenAM properties. A custom
 attribute mapper can be provided.<br/><br/>A custom attribute mapper must implement the
 <code>org.forgerock.openam.authentication.modules.common.mapping.AttributeMapper</code>
 interface.<br/>Provided implementations
 are:<ul><li>org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper</
li><li>org.forgerock.openam.authentication.modules.oidc.JwtAttributeMapper (can only be used when
 using the openid scope)</li></ul>String constructor parameters can be provided by appending <code>|</
code> separated values.",
              "propertyOrder" : 1700,
              "required" : true,
              "items" : {
                "type" : "string"
              },
              "type" : "array",
              "exampleValue" : ""
            },
            "accountMapperConfiguration" : {
              "title" : "Account Mapper Configuration",
              "description" : "Mapping of OAuth account to local OpenAM account<br><br>Attribute
 configuration that will be used to map the account of the user authenticated in the OAuth 2.0
 Provider to the local data store in the OpenAM. Example: <code>OAuth2.0_attribute=local_attribute</
code>",
              "propertyOrder" : 1600,
              "required" : true,
              "items" : {
                "type" : "string"
              },
              "type" : "array",
              "exampleValue" : ""
            },
            "createAccount" : {
              "title" : "Create account if it does not exist",
              "description" : "If the OAuth2 account does not exist in the local OpenAM data store,
 an account will be created dynamically.<br><br>If this is enabled, the account mapper could create
 the account dynamically if there is no account mapped. Before creating the account, a dialog
 prompting for a password and asking for an activation code can be shown if the parameter \"Prompt
```

```
 for password setting and activation code\" is enabled.<br /><br />If this flag is not enabled, 3
 alternative options exist:<br/><br/><ol><li>The accounts need to have a user profile in the OpenAM
 User Data Store</li><li>The user does not have a user profile and the \"Ignore Profile\" is set in
 the Authentication Service of the realm.</li><li>The account is mapped to an anonymous account (see
 parameter \"Map to anonymous user\" and \"Anonymous User\")</li></ol>",
              "propertyOrder" : 1360,
              "required" : true,
              "type" : "boolean",
              "exampleValue" : ""
            },
            "enableRegistrationService" : {
              "title" : "Use IDM as Registration Service",
              "description" : "Whether to use IDM as an external Registration Service to
 complete registration for new users.<br><br>IDM is called and passed these parameters:<br/><br/
><ul><li><code>clientToken</code>: Signed, encrypted JWT of the OAuth 2.0 authentication state.</
li><li><code>returnParams</code>: Encoded URL parameters, required to be returned to AM to resume
 authentication after registration in IDM is complete.</li></ul>",
              "propertyOrder" : 1350,
              "required" : true,
              "type" : "boolean",
              "exampleValue" : ""
            },
            "anonymousUserName" : {
              "title" : "Anonymous User",
              "description" : "Username of the OpenAM anonymous user<br><br>The username of the user
 that will represent the anonymous user. This user account must already exist in the realm.",
              "propertyOrder" : 2100,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            }
          }
        },
        "emailSettings" : {
          "type" : "object",
          "title" : "Email",
          "propertyOrder" : 2,
          "properties" : {
            "smtpFromAddress" : {
              "title" : "SMTP From address",
              "description" : "The email address on behalf of whom the messages will be sent",
              "propertyOrder" : 1945,
              "required" : true,
              "type" : "string",
              "exampleValue" : "info@forgerock.com"
            },
            "smtpPassword" : {
              "title" : "SMTP User Password",
              "description" : "The Password of the SMTP User Name",
              "propertyOrder" : 1935,
              "required" : true,
              "type" : "string",
              "format" : "password",
              "exampleValue" : ""
            },
            "smtpHost" : {
              "title" : "SMTP host",
              "description" : "The mail host that will be used by the Email Gateway implementation",
              "propertyOrder" : 1920,
```

```
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            },
            "smtpUsername" : {
              "title" : "SMTP User Name",
              "description" : "If the SMTP Service requires authentication, configure the user name
here",
              "propertyOrder" : 1930,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            },
            "emailAttribute" : {
              "title" : "Email attribute in the Response",
              "description" : "Attribute from the response used to send activation code
emails.<br><br>The attribute in the response from the profile service of the Provider that contains
the email address of the authenticated user. This address will be used to send an email with an
activation code when the accounts are allowed to be created dynamically.",
              "propertyOrder" : 1910,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            },
            "smtpSslEnabled" : {
              "title" : "SMTP SSL Enabled",
              "description" : "Tick this option if the SMTP Server provides SSL",
              "propertyOrder" : 1940,
              "required" : true,
              "type" : "boolean",
              "exampleValue" : ""
            },
            "smtpPort" : {
              "title" : "SMTP port",
              "description" : "The TCP port that will be used by the SMTP gateway",
              "propertyOrder" : 1925,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            },
            "emailGateway" : {
              "title" : "Mail Server Gateway implementation class",
              "description" : "The class used by the module to send
email.<br><br>This class is used by the module to send email. A custom
implementation can be provided.<br/><br/>The custom implementation must implement the
<code>org.forgerock.openam.authentication.modules.oauth2.EmailGateway</code>",
              "propertyOrder" : 1915,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            }
          }
        },
        "core" : {
          "type" : "object",
          "title" : "Core",
          "propertyOrder" : 0,
          "properties" : {
            "provider" : {
```

```
              "title" : "Social Provider",
              "description" : "Social Provider for which this module is being setup.",
              "propertyOrder" : 200,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            },
            "ssoProxyUrl" : {
              "title" : "Proxy URL",
              "description" : "The URL to the OpenAM OAuth proxy JSP<br><br>This URL should only be
changed from the default, if an external server is performing the GET to POST proxying. The default
is <code>/openam/oauth2c/OAuthProxy.jsp</code>",
              "propertyOrder" : 1300,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            },
            "authenticationLevel" : {
              "title" : "Authentication Level",
              "description" : "The authentication level associated with this module.<br><br>Each
authentication module has an authentication level that can be used to indicate the level of security
associated with the module; 0 is the lowest (and the default).",
              "propertyOrder" : 100,
              "required" : true,
              "type" : "integer",
              "exampleValue" : ""
            },
            "subjectProperty" : {
              "title" : "Subject Property",
              "description" : "Property used to identify which attribute an auth server identifies a
user by.",
              "propertyOrder" : 1100,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            },
            "scope" : {
              "title" : "Scope",
              "description" : "OAuth scope; list of user profile properties<br><br>According to the
OAuth 2.0 Authorization Framework, scope is a space-separated list of user profile attributes that
the client application requires. The list depends on the permissions that the resource owner grants
to the client application.<br/><br/> Some authorization servers use non-standard separators for
scopes. For example, Facebook takes a comma-separated list.<br/><br/>",
              "propertyOrder" : 900,
              "required" : true,
              "items" : {
                "type" : "string"
              },
              "type" : "array",
              "exampleValue" : ""
            },
            "userInfoEndpoint" : {
              "title" : "User Profile Service URL",
              "description" : "User profile information URL<br><br>This URL endpoint provides user
profile information and is provided by the OAuth Identity Provider<br/><br/><i>NB </i>This URL should
return JSON objects in response",
              "propertyOrder" : 800,
              "required" : true,
              "type" : "string",
```

```
              "exampleValue" : ""
            }
          }
        }
      },
      "type" : "object",
      "title" : "Realm Defaults"
    }
  }
}
```

SocialAuthWeChatModule

Realm Operations

Resource path: `/realm-config/authentication/modules/authSocialWeChat`

Resource version: `1.0`

create

Usage:

```
am> create SocialAuthWeChatModule --realm Realm --id id --body body
```

Parameters:

`--id`

The unique identifier for the resource.

`--body`

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "accountProvisioning" : {
      "type" : "object",
      "title" : "Account Provisioning",
      "propertyOrder" : 1,
      "properties" : {
        "accountMapperClass" : {
          "title" : "Account Mapper",
          "description" : "Name of the class implementing the attribute mapping for the
 account search.<br><br>This class is used by the module to map from the account information
 received from the OAuth Identity Provider into OpenAM.<br/><br/>The class must implement
 the <code>org.forgerock.openam.authentication.modules.common.mapping.AttributeMapper</code>
 interface.<br/>Provided implementations
 are:<ul><li>org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper</
```

```
li><li>org.forgerock.openam.authentication.modules.oidc.JwtAttributeMapper (can only be used when
 using the openid scope)</li></ul>String constructor parameters can be provided by appending <code>|</
code> separated values.",
          "propertyOrder" : 1500,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "accountMapperConfiguration" : {
          "title" : "Account Mapper Configuration",
          "description" : "Mapping of OAuth account to local OpenAM account<br><br>Attribute
 configuration that will be used to map the account of the user authenticated in the OAuth 2.0
 Provider to the local data store in the OpenAM. Example: <code>OAuth2.0_attribute=local_attribute</
code>",
          "propertyOrder" : 1600,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "attributeMappingClasses" : {
          "title" : "Attribute Mapper",
          "description" : "Name of the class that implements the attribute
 mapping<br><br>This class maps the OAuth properties into OpenAM properties. A custom
 attribute mapper can be provided.<br/><br/>A custom attribute mapper must implement the
 <code>org.forgerock.openam.authentication.modules.common.mapping.AttributeMapper</code>
 interface.<br/>Provided implementations
 are:<ul><li>org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper</
li><li>org.forgerock.openam.authentication.modules.oidc.JwtAttributeMapper (can only be used when
 using the openid scope)</li></ul>String constructor parameters can be provided by appending <code>|</
code> separated values.",
          "propertyOrder" : 1700,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "createAccount" : {
          "title" : "Create account if it does not exist",
          "description" : "If the OAuth2 account does not exist in the local OpenAM data store, an
 account will be created dynamically.<br><br>If this is enabled, the account mapper could create
 the account dynamically if there is no account mapped. Before creating the account, a dialog
 prompting for a password and asking for an activation code can be shown if the parameter \"Prompt
 for password setting and activation code\" is enabled.<br /><br />If this flag is not enabled, 3
 alternative options exist:<br/><br/><ol><li>The accounts need to have a user profile in the OpenAM
 User Data Store</li><li>The user does not have a user profile and the \"Ignore Profile\" is set in
 the Authentication Service of the realm.</li><li>The account is mapped to an anonymous account (see
 parameter \"Map to anonymous user\" and \"Anonymous User\")</li></ol>",
          "propertyOrder" : 1360,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "enableRegistrationService" : {
          "title" : "Use IDM as Registration Service",
```

```
          "description" : "Whether to use IDM as an external Registration Service to complete
 registration for new users.<br><br>IDM is called and passed these parameters:<br/><br/
><ul><li><code>clientToken</code>: Signed, encrypted JWT of the OAuth 2.0 authentication state.</
li><li><code>returnParams</code>: Encoded URL parameters, required to be returned to AM to resume
 authentication after registration in IDM is complete.</li></ul>",
          "propertyOrder" : 1350,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "promptPasswordFlag" : {
          "title" : "Prompt for password setting and activation code",
          "description" : "Users must set a password and complete the activation flow during dynamic
 profile creation.<br><br>If this is enabled, the user must set a password before the system creates
 an account dynamically and an activation code will be sent to the user's email address. The account
 will be created only if the password and activation code are properly set. <br />If this is disabled,
 the account will be created transparently without prompting the user.",
          "propertyOrder" : 1905,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "saveAttributesInSession" : {
          "title" : "Save attributes in the session",
          "description" : "If this option is enabled, the attributes configured in the attribute
 mapper will be saved into the OpenAM session",
          "propertyOrder" : 2400,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "accountProviderClass" : {
          "title" : "Account Provider",
          "description" : "Name of the class implementing the account provider.<br><br>This
 class is used by the module to find the account from the attributes mapped by the Account
 Mapper <code>org.forgerock.openam.authentication.modules.common.mapping.AccountProvider</code>
 interface.<br/>String constructor parameters can be provided by appending <code>|</code> separated
 values.",
          "propertyOrder" : 1400,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "mapToAnonymousUser" : {
          "title" : "Map to anonymous user",
          "description" : "Enabled anonymous user access to OpenAM for OAuth authenticated
 users<br><br>If selected, the authenticated users in the OAuth 2.0 Provider will be mapped to the
 anonymous user configured in the next parameter.<br/>If not selected the users authenticated will be
 mapped by the parameters configured in the account mapper.<br/><br/><i>NB </i>If <i>Create account if
 it does not exist</i> is enabled, that parameter takes precedence.",
          "propertyOrder" : 2000,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "anonymousUserName" : {
          "title" : "Anonymous User",
          "description" : "Username of the OpenAM anonymous user<br><br>The username of the user that
 will represent the anonymous user. This user account must already exist in the realm.",
```

```
          "propertyOrder" : 2100,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "attributeMapperConfiguration" : {
          "title" : "Attribute Mapper Configuration",
          "description" : "Mapping of OAuth attributes to local OpenAM attributes<br><br>Attribute
 configuration that will be used to map the user info obtained from the OAuth 2.0 Provider to the
 local user data store in the OpenAM.<br/><br/>Example: <code>OAuth2.0_attribute=local_attribute</
code>",
          "propertyOrder" : 1800,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        }
      }
    },
    "core" : {
      "type" : "object",
      "title" : "Core",
      "propertyOrder" : 0,
      "properties" : {
        "authenticationLevel" : {
          "title" : "Authentication Level",
          "description" : "The authentication level associated with this module.<br><br>Each
 authentication module has an authentication level that can be used to indicate the level of security
 associated with the module; 0 is the lowest (and the default).",
          "propertyOrder" : 100,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "clientSecret" : {
          "title" : "Client Secret",
          "description" : "OAuth client_secret parameter<br><br>For more information on the OAuth
 client_secret parameter refer to the <a href=\"http://tools.ietf.org/html/rfc6749#section-2.3.1\"
 target=\"_blank\">RFC 6749</a>, section 2.3.1",
          "propertyOrder" : 500,
          "required" : true,
          "type" : "string",
          "format" : "password",
          "exampleValue" : ""
        },
        "provider" : {
          "title" : "Social Provider",
          "description" : "Social Provider for which this module is being setup.",
          "propertyOrder" : 200,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "usesBasicAuth" : {
          "title" : "Use Basic Auth",
          "description" : "When enabled, the client will use basic auth for authenticating with  the
 social auth provider. Enabled by default.",
```

```
          "propertyOrder" : 1200,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "authorizeEndpoint" : {
          "title" : "Authentication Endpoint URL",
          "description" : "OAuth authentication endpoint URL<br><br>This is the URL endpoint for OAuth
 authentication provided by the OAuth Identity Provider",
          "propertyOrder" : 600,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "clientId" : {
          "title" : "Client Id",
          "description" : "OAuth client_id parameter<br><br>For more information on the OAuth
 client_id parameter refer to the <a href=\"http://tools.ietf.org/html/rfc6749#section-2.3.1\" target=
\"_blank\">RFC 6749</a>, section 2.3.1",
          "propertyOrder" : 400,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "subjectProperty" : {
          "title" : "Subject Property",
          "description" : "Property used to identify which attribute an auth server identifies a user
 by.",
          "propertyOrder" : 1100,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "ssoProxyUrl" : {
          "title" : "Proxy URL",
          "description" : "The URL to the OpenAM OAuth proxy JSP<br><br>This URL should only be
 changed from the default, if an external server is performing the GET to POST proxying. The default
 is <code>/openam/oauth2c/OAuthProxy.jsp</code>",
          "propertyOrder" : 1300,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "scope" : {
          "title" : "Scope",
          "description" : "OAuth scope; list of user profile properties<br><br>According to the OAuth
 2.0 Authorization Framework, scope is a space-separated list of user profile attributes that the
 client application requires. The list depends on the permissions that the resource owner grants to
 the client application.<br/><br/> Some authorization servers use non-standard separators for scopes.
 For example, Facebook takes a comma-separated list.<br/><br/>",
          "propertyOrder" : 900,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "minItems" : 1,
          "type" : "array",
          "exampleValue" : ""
        },
```

```
        "tokenEndpoint" : {
          "title" : "Access Token Endpoint URL",
          "description" : "OAuth access token endpoint URL<br><br>This is the URL endpoint for
 access token retrieval provided by the OAuth Identity Provider. Refer to the <a href=\"http://
tools.ietf.org/html/rfc6749#section-3.2\" target=\"_blank\">RFC 6749</a>, section 3.2",
          "propertyOrder" : 700,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "scopeDelimiter" : {
          "title" : "Scope Delimiter",
          "description" : "Delimiter used to separate scope values. Default value is space.",
          "propertyOrder" : 1000,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "userInfoEndpoint" : {
          "title" : "User Profile Service URL",
          "description" : "User profile information URL<br><br>This URL endpoint provides user profile
 information and is provided by the OAuth Identity Provider<br/><br/><i>NB </i>This URL should return
 JSON objects in response",
          "propertyOrder" : 800,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "emailSettings" : {
      "type" : "object",
      "title" : "Email",
      "propertyOrder" : 2,
      "properties" : {
        "smtpFromAddress" : {
          "title" : "SMTP From address",
          "description" : "The email address on behalf of whom the messages will be sent",
          "propertyOrder" : 1945,
          "required" : true,
          "type" : "string",
          "exampleValue" : "info@forgerock.com"
        },
        "smtpHost" : {
          "title" : "SMTP host",
          "description" : "The mail host that will be used by the Email Gateway implementation",
          "propertyOrder" : 1920,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "emailGateway" : {
          "title" : "Mail Server Gateway implementation class",
          "description" : "The class used by the module to send email.<br><br>This class is used by
 the module to send email. A custom implementation can be provided.<br/><br/>The custom implementation
 must implement the <code>org.forgerock.openam.authentication.modules.oauth2.EmailGateway</code>",
          "propertyOrder" : 1915,
          "required" : true,
          "type" : "string",
```

```
          "exampleValue" : ""
        },
        "smtpPort" : {
          "title" : "SMTP port",
          "description" : "The TCP port that will be used by the SMTP gateway",
          "propertyOrder" : 1925,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "smtpSslEnabled" : {
          "title" : "SMTP SSL Enabled",
          "description" : "Tick this option if the SMTP Server provides SSL",
          "propertyOrder" : 1940,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "smtpUsername" : {
          "title" : "SMTP User Name",
          "description" : "If the SMTP Service requires authentication, configure the user name here",
          "propertyOrder" : 1930,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "smtpPassword" : {
          "title" : "SMTP User Password",
          "description" : "The Password of the SMTP User Name",
          "propertyOrder" : 1935,
          "required" : true,
          "type" : "string",
          "format" : "password",
          "exampleValue" : ""
        },
        "emailAttribute" : {
          "title" : "Email attribute in the Response",
          "description" : "Attribute from the response used to send activation code emails.<br><br>The
 attribute in the response from the profile service of the Provider that contains the email address of
 the authenticated user. This address will be used to send an email with an activation code when the
 accounts are allowed to be created dynamically.",
          "propertyOrder" : 1910,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    }
  }
}
```

delete

Usage:

```
am> delete SocialAuthWeChatModule --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action SocialAuthWeChatModule --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action SocialAuthWeChatModule --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action SocialAuthWeChatModule --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query SocialAuthWeChatModule --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read SocialAuthWeChatModule --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update SocialAuthWeChatModule --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "accountProvisioning" : {
      "type" : "object",
      "title" : "Account Provisioning",
      "propertyOrder" : 1,
      "properties" : {
        "accountMapperClass" : {
          "title" : "Account Mapper",
          "description" : "Name of the class implementing the attribute mapping for the
 account search.<br><br>This class is used by the module to map from the account information
 received from the OAuth Identity Provider into OpenAM.<br/><br/>The class must implement
 the <code>org.forgerock.openam.authentication.modules.common.mapping.AttributeMapper</code>
 interface.<br/>Provided implementations
 are:<ul><li>org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper</
li><li>org.forgerock.openam.authentication.modules.oidc.JwtAttributeMapper (can only be used when
 using the openid scope)</li></ul>String constructor parameters can be provided by appending <code>|</
code> separated values.",
          "propertyOrder" : 1500,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "accountMapperConfiguration" : {
          "title" : "Account Mapper Configuration",
          "description" : "Mapping of OAuth account to local OpenAM account<br><br>Attribute
 configuration that will be used to map the account of the user authenticated in the OAuth 2.0
 Provider to the local data store in the OpenAM. Example: <code>OAuth2.0_attribute=local_attribute</
code>",
          "propertyOrder" : 1600,
          "required" : true,
          "items" : {
            "type" : "string"
```

```
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "attributeMappingClasses" : {
          "title" : "Attribute Mapper",
          "description" : "Name of the class that implements the attribute
 mapping<br><br>This class maps the OAuth properties into OpenAM properties. A custom
 attribute mapper can be provided.<br/><br/>A custom attribute mapper must implement the
 <code>org.forgerock.openam.authentication.modules.common.mapping.AttributeMapper</code>
 interface.<br/>Provided implementations
 are:<ul><li>org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper</
li><li>org.forgerock.openam.authentication.modules.oidc.JwtAttributeMapper (can only be used when
 using the openid scope)</li></ul>String constructor parameters can be provided by appending <code>|</
code> separated values.",
          "propertyOrder" : 1700,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "createAccount" : {
          "title" : "Create account if it does not exist",
          "description" : "If the OAuth2 account does not exist in the local OpenAM data store, an
 account will be created dynamically.<br><br>If this is enabled, the account mapper could create
 the account dynamically if there is no account mapped. Before creating the account, a dialog
 prompting for a password and asking for an activation code can be shown if the parameter \"Prompt
 for password setting and activation code\" is enabled.<br /><br />If this flag is not enabled, 3
 alternative options exist:<br/><br/><ol><li>The accounts need to have a user profile in the OpenAM
 User Data Store</li><li>The user does not have a user profile and the \"Ignore Profile\" is set in
 the Authentication Service of the realm.</li><li>The account is mapped to an anonymous account (see
 parameter \"Map to anonymous user\" and \"Anonymous User\")</li></ol>",
          "propertyOrder" : 1360,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "enableRegistrationService" : {
          "title" : "Use IDM as Registration Service",
          "description" : "Whether to use IDM as an external Registration Service to complete
 registration for new users.<br><br>IDM is called and passed these parameters:<br/><br/
><ul><li><code>clientToken</code>: Signed, encrypted JWT of the OAuth 2.0 authentication state.</
li><li><code>returnParams</code>: Encoded URL parameters, required to be returned to AM to resume
 authentication after registration in IDM is complete.</li></ul>",
          "propertyOrder" : 1350,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "promptPasswordFlag" : {
          "title" : "Prompt for password setting and activation code",
          "description" : "Users must set a password and complete the activation flow during dynamic
 profile creation.<br><br>If this is enabled, the user must set a password before the system creates
 an account dynamically and an activation code will be sent to the user's email address. The account
 will be created only if the password and activation code are properly set. <br />If this is disabled,
 the account will be created transparently without prompting the user.",
          "propertyOrder" : 1905,
```

```
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "saveAttributesInSession" : {
          "title" : "Save attributes in the session",
          "description" : "If this option is enabled, the attributes configured in the attribute
 mapper will be saved into the OpenAM session",
          "propertyOrder" : 2400,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "accountProviderClass" : {
          "title" : "Account Provider",
          "description" : "Name of the class implementing the account provider.<br><br>This
 class is used by the module to find the account from the attributes mapped by the Account
 Mapper <code>org.forgerock.openam.authentication.modules.common.mapping.AccountProvider</code>
 interface.<br/>String constructor parameters can be provided by appending <code>|</code> separated
 values.",
          "propertyOrder" : 1400,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "mapToAnonymousUser" : {
          "title" : "Map to anonymous user",
          "description" : "Enabled anonymous user access to OpenAM for OAuth authenticated
 users<br><br>If selected, the authenticated users in the OAuth 2.0 Provider will be mapped to the
 anonymous user configured in the next parameter.<br/>If not selected the users authenticated will be
 mapped by the parameters configured in the account mapper.<br/><br/><i>NB </i>If <i>Create account if
 it does not exist</i> is enabled, that parameter takes precedence.",
          "propertyOrder" : 2000,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "anonymousUserName" : {
          "title" : "Anonymous User",
          "description" : "Username of the OpenAM anonymous user<br><br>The username of the user that
 will represent the anonymous user. This user account must already exist in the realm.",
          "propertyOrder" : 2100,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "attributeMapperConfiguration" : {
          "title" : "Attribute Mapper Configuration",
          "description" : "Mapping of OAuth attributes to local OpenAM attributes<br><br>Attribute
 configuration that will be used to map the user info obtained from the OAuth 2.0 Provider to the
 local user data store in the OpenAM.<br/><br/>Example: <code>OAuth2.0_attribute=local_attribute</
code>",
          "propertyOrder" : 1800,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
```

```
        }
      }
    },
    "core" : {
      "type" : "object",
      "title" : "Core",
      "propertyOrder" : 0,
      "properties" : {
        "authenticationLevel" : {
          "title" : "Authentication Level",
          "description" : "The authentication level associated with this module.<br><br>Each
authentication module has an authentication level that can be used to indicate the level of security
associated with the module; 0 is the lowest (and the default).",
          "propertyOrder" : 100,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "clientSecret" : {
          "title" : "Client Secret",
          "description" : "OAuth client_secret parameter<br><br>For more information on the OAuth
client_secret parameter refer to the <a href=\"http://tools.ietf.org/html/rfc6749#section-2.3.1\"
target=\"_blank\">RFC 6749</a>, section 2.3.1",
          "propertyOrder" : 500,
          "required" : true,
          "type" : "string",
          "format" : "password",
          "exampleValue" : ""
        },
        "provider" : {
          "title" : "Social Provider",
          "description" : "Social Provider for which this module is being setup.",
          "propertyOrder" : 200,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "usesBasicAuth" : {
          "title" : "Use Basic Auth",
          "description" : "When enabled, the client will use basic auth for authenticating with  the
social auth provider. Enabled by default.",
          "propertyOrder" : 1200,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "authorizeEndpoint" : {
          "title" : "Authentication Endpoint URL",
          "description" : "OAuth authentication endpoint URL<br><br>This is the URL endpoint for OAuth
authentication provided by the OAuth Identity Provider",
          "propertyOrder" : 600,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "clientId" : {
          "title" : "Client Id",
```

```
          "description" : "OAuth client_id parameter<br><br>For more information on the OAuth
 client_id parameter refer to the <a href=\"http://tools.ietf.org/html/rfc6749#section-2.3.1\" target=
\"_blank\">RFC 6749</a>, section 2.3.1",
          "propertyOrder" : 400,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "subjectProperty" : {
          "title" : "Subject Property",
          "description" : "Property used to identify which attribute an auth server identifies a user
 by.",
          "propertyOrder" : 1100,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "ssoProxyUrl" : {
          "title" : "Proxy URL",
          "description" : "The URL to the OpenAM OAuth proxy JSP<br><br>This URL should only be
 changed from the default, if an external server is performing the GET to POST proxying. The default
 is <code>/openam/oauth2c/OAuthProxy.jsp</code>",
          "propertyOrder" : 1300,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "scope" : {
          "title" : "Scope",
          "description" : "OAuth scope; list of user profile properties<br><br>According to the OAuth
 2.0 Authorization Framework, scope is a space-separated list of user profile attributes that the
 client application requires. The list depends on the permissions that the resource owner grants to
 the client application.<br/><br/> Some authorization servers use non-standard separators for scopes.
 For example, Facebook takes a comma-separated list.<br/><br/>",
          "propertyOrder" : 900,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "minItems" : 1,
          "type" : "array",
          "exampleValue" : ""
        },
        "tokenEndpoint" : {
          "title" : "Access Token Endpoint URL",
          "description" : "OAuth access token endpoint URL<br><br>This is the URL endpoint for
 access token retrieval provided by the OAuth Identity Provider. Refer to the <a href=\"http://
tools.ietf.org/html/rfc6749#section-3.2\" target=\"_blank\">RFC 6749</a>, section 3.2",
          "propertyOrder" : 700,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "scopeDelimiter" : {
          "title" : "Scope Delimiter",
          "description" : "Delimiter used to separate scope values. Default value is space.",
          "propertyOrder" : 1000,
          "required" : true,
          "type" : "string",
```

```
          "exampleValue" : ""
        },
        "userInfoEndpoint" : {
          "title" : "User Profile Service URL",
          "description" : "User profile information URL<br><br>This URL endpoint provides user profile
information and is provided by the OAuth Identity Provider<br/><br/><i>NB </i>This URL should return
JSON objects in response",
          "propertyOrder" : 800,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "emailSettings" : {
      "type" : "object",
      "title" : "Email",
      "propertyOrder" : 2,
      "properties" : {
        "smtpFromAddress" : {
          "title" : "SMTP From address",
          "description" : "The email address on behalf of whom the messages will be sent",
          "propertyOrder" : 1945,
          "required" : true,
          "type" : "string",
          "exampleValue" : "info@forgerock.com"
        },
        "smtpHost" : {
          "title" : "SMTP host",
          "description" : "The mail host that will be used by the Email Gateway implementation",
          "propertyOrder" : 1920,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "emailGateway" : {
          "title" : "Mail Server Gateway implementation class",
          "description" : "The class used by the module to send email.<br><br>This class is used by
the module to send email. A custom implementation can be provided.<br/><br/>The custom implementation
must implement the <code>org.forgerock.openam.authentication.modules.oauth2.EmailGateway</code>",
          "propertyOrder" : 1915,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "smtpPort" : {
          "title" : "SMTP port",
          "description" : "The TCP port that will be used by the SMTP gateway",
          "propertyOrder" : 1925,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "smtpSslEnabled" : {
          "title" : "SMTP SSL Enabled",
          "description" : "Tick this option if the SMTP Server provides SSL",
          "propertyOrder" : 1940,
          "required" : true,
          "type" : "boolean",
```

```
          "exampleValue" : ""
        },
        "smtpUsername" : {
          "title" : "SMTP User Name",
          "description" : "If the SMTP Service requires authentication, configure the user name here",
          "propertyOrder" : 1930,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "smtpPassword" : {
          "title" : "SMTP User Password",
          "description" : "The Password of the SMTP User Name",
          "propertyOrder" : 1935,
          "required" : true,
          "type" : "string",
          "format" : "password",
          "exampleValue" : ""
        },
        "emailAttribute" : {
          "title" : "Email attribute in the Response",
          "description" : "Attribute from the response used to send activation code emails.<br><br>The
 attribute in the response from the profile service of the Provider that contains the email address of
 the authenticated user. This address will be used to send an email with an activation code when the
 accounts are allowed to be created dynamically.",
          "propertyOrder" : 1910,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    }
  }
}
```


Global Operations

Resource path: `/global-config/authentication/modules/authSocialWeChat`

Resource version: `1.0`

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action SocialAuthWeChatModule --global --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action SocialAuthWeChatModule --global --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action SocialAuthWeChatModule --global --actionName nextdescendents
```

read

Usage:

```
am> read SocialAuthWeChatModule --global
```

update

Usage:

```
am> update SocialAuthWeChatModule --global --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "defaults" : {
      "properties" : {
        "emailSettings" : {
          "type" : "object",
          "title" : "Email",
          "propertyOrder" : 2,
          "properties" : {
            "emailGateway" : {
              "title" : "Mail Server Gateway implementation class",
              "description" : "The class used by the module to send
email.<br><br>This class is used by the module to send email. A custom
implementation can be provided.<br/><br/>The custom implementation must implement the
<code>org.forgerock.openam.authentication.modules.oauth2.EmailGateway</code>",
              "propertyOrder" : 1915,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            },
            "smtpSslEnabled" : {
              "title" : "SMTP SSL Enabled",
```

```
              "description" : "Tick this option if the SMTP Server provides SSL",
              "propertyOrder" : 1940,
              "required" : true,
              "type" : "boolean",
              "exampleValue" : ""
            },
            "smtpUsername" : {
              "title" : "SMTP User Name",
              "description" : "If the SMTP Service requires authentication, configure the user name
here",
              "propertyOrder" : 1930,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            },
            "smtpPort" : {
              "title" : "SMTP port",
              "description" : "The TCP port that will be used by the SMTP gateway",
              "propertyOrder" : 1925,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            },
            "smtpPassword" : {
              "title" : "SMTP User Password",
              "description" : "The Password of the SMTP User Name",
              "propertyOrder" : 1935,
              "required" : true,
              "type" : "string",
              "format" : "password",
              "exampleValue" : ""
            },
            "emailAttribute" : {
              "title" : "Email attribute in the Response",
              "description" : "Attribute from the response used to send activation code
emails.<br><br>The attribute in the response from the profile service of the Provider that contains
the email address of the authenticated user. This address will be used to send an email with an
activation code when the accounts are allowed to be created dynamically.",
              "propertyOrder" : 1910,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            },
            "smtpFromAddress" : {
              "title" : "SMTP From address",
              "description" : "The email address on behalf of whom the messages will be sent",
              "propertyOrder" : 1945,
              "required" : true,
              "type" : "string",
              "exampleValue" : "info@forgerock.com"
            },
            "smtpHost" : {
              "title" : "SMTP host",
              "description" : "The mail host that will be used by the Email Gateway implementation",
              "propertyOrder" : 1920,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            }
```

```
          }
        },
        "accountProvisioning" : {
          "type" : "object",
          "title" : "Account Provisioning",
          "propertyOrder" : 1,
          "properties" : {
            "anonymousUserName" : {
              "title" : "Anonymous User",
              "description" : "Username of the OpenAM anonymous user<br><br>The username of the user
 that will represent the anonymous user. This user account must already exist in the realm.",
              "propertyOrder" : 2100,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            },
            "saveAttributesInSession" : {
              "title" : "Save attributes in the session",
              "description" : "If this option is enabled, the attributes configured in the attribute
 mapper will be saved into the OpenAM session",
              "propertyOrder" : 2400,
              "required" : true,
              "type" : "boolean",
              "exampleValue" : ""
            },
            "accountMapperConfiguration" : {
              "title" : "Account Mapper Configuration",
              "description" : "Mapping of OAuth account to local OpenAM account<br><br>Attribute
 configuration that will be used to map the account of the user authenticated in the OAuth 2.0
 Provider to the local data store in the OpenAM. Example: <code>OAuth2.0_attribute=local_attribute</
code>",
              "propertyOrder" : 1600,
              "required" : true,
              "items" : {
                "type" : "string"
              },
              "type" : "array",
              "exampleValue" : ""
            },
            "mapToAnonymousUser" : {
              "title" : "Map to anonymous user",
              "description" : "Enabled anonymous user access to OpenAM for OAuth authenticated
 users<br><br>If selected, the authenticated users in the OAuth 2.0 Provider will be mapped to the
 anonymous user configured in the next parameter.<br/>If not selected the users authenticated will be
 mapped by the parameters configured in the account mapper.<br/><br/><i>NB </i>If <i>Create account if
 it does not exist</i> is enabled, that parameter takes precedence.",
              "propertyOrder" : 2000,
              "required" : true,
              "type" : "boolean",
              "exampleValue" : ""
            },
            "attributeMapperConfiguration" : {
              "title" : "Attribute Mapper Configuration",
              "description" : "Mapping of OAuth attributes to local OpenAM attributes<br><br>Attribute
 configuration that will be used to map the user info obtained from the OAuth 2.0 Provider to the
 local user data store in the OpenAM.<br/><br/>Example: <code>OAuth2.0_attribute=local_attribute</
code>",
              "propertyOrder" : 1800,
              "required" : true,
```

```
              "items" : {
                "type" : "string"
              },
              "type" : "array",
              "exampleValue" : ""
            },
            "promptPasswordFlag" : {
              "title" : "Prompt for password setting and activation code",
              "description" : "Users must set a password and complete the activation flow during
 dynamic profile creation.<br><br>If this is enabled, the user must set a password before the system
 creates an account dynamically and an activation code will be sent to the user's email address. The
 account will be created only if the password and activation code are properly set. <br />If this is
 disabled, the account will be created transparently without prompting the user.",
              "propertyOrder" : 1905,
              "required" : true,
              "type" : "boolean",
              "exampleValue" : ""
            },
            "createAccount" : {
              "title" : "Create account if it does not exist",
              "description" : "If the OAuth2 account does not exist in the local OpenAM data store,
 an account will be created dynamically.<br><br>If this is enabled, the account mapper could create
 the account dynamically if there is no account mapped. Before creating the account, a dialog
 prompting for a password and asking for an activation code can be shown if the parameter \"Prompt
 for password setting and activation code\" is enabled.<br /><br />If this flag is not enabled, 3
 alternative options exist:<br/><br/><ol><li>The accounts need to have a user profile in the OpenAM
 User Data Store</li><li>The user does not have a user profile and the \"Ignore Profile\" is set in
 the Authentication Service of the realm.</li><li>The account is mapped to an anonymous account (see
 parameter \"Map to anonymous user\" and \"Anonymous User\")</li></ol>",
              "propertyOrder" : 1360,
              "required" : true,
              "type" : "boolean",
              "exampleValue" : ""
            },
            "attributeMappingClasses" : {
              "title" : "Attribute Mapper",
              "description" : "Name of the class that implements the attribute
 mapping<br><br>This class maps the OAuth properties into OpenAM properties. A custom
 attribute mapper can be provided.<br/><br/>A custom attribute mapper must implement the
 <code>org.forgerock.openam.authentication.modules.common.mapping.AttributeMapper</code>
 interface.<br/>Provided implementations
 are:<ul><li>org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper</
li><li>org.forgerock.openam.authentication.modules.oidc.JwtAttributeMapper (can only be used when
 using the openid scope)</li></ul>String constructor parameters can be provided by appending <code>|</
code> separated values.",
              "propertyOrder" : 1700,
              "required" : true,
              "items" : {
                "type" : "string"
              },
              "type" : "array",
              "exampleValue" : ""
            },
            "accountMapperClass" : {
              "title" : "Account Mapper",
              "description" : "Name of the class implementing the attribute mapping for the
 account search.<br><br>This class is used by the module to map from the account information
 received from the OAuth Identity Provider into OpenAM.<br/><br/>The class must implement
 the <code>org.forgerock.openam.authentication.modules.common.mapping.AttributeMapper</code>
```

```
 interface.<br/>Provided implementations
 are:<ul><li>org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper</
li><li>org.forgerock.openam.authentication.modules.oidc.JwtAttributeMapper (can only be used when
 using the openid scope)</li></ul>String constructor parameters can be provided by appending <code>|</
code> separated values.",
              "propertyOrder" : 1500,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            },
            "enableRegistrationService" : {
              "title" : "Use IDM as Registration Service",
              "description" : "Whether to use IDM as an external Registration Service to
 complete registration for new users.<br><br>IDM is called and passed these parameters:<br/><br/
><ul><li><code>clientToken</code>: Signed, encrypted JWT of the OAuth 2.0 authentication state.</
li><li><code>returnParams</code>: Encoded URL parameters, required to be returned to AM to resume
 authentication after registration in IDM is complete.</li></ul>",
              "propertyOrder" : 1350,
              "required" : true,
              "type" : "boolean",
              "exampleValue" : ""
            },
            "accountProviderClass" : {
              "title" : "Account Provider",
              "description" : "Name of the class implementing the account provider.<br><br>This
 class is used by the module to find the account from the attributes mapped by the Account
 Mapper <code>org.forgerock.openam.authentication.modules.common.mapping.AccountProvider</code>
 interface.<br/>String constructor parameters can be provided by appending <code>|</code> separated
 values.",
              "propertyOrder" : 1400,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            }
          }
        },
        "core" : {
          "type" : "object",
          "title" : "Core",
          "propertyOrder" : 0,
          "properties" : {
            "tokenEndpoint" : {
              "title" : "Access Token Endpoint URL",
              "description" : "OAuth access token endpoint URL<br><br>This is the URL endpoint for
 access token retrieval provided by the OAuth Identity Provider. Refer to the <a href=\"http://
tools.ietf.org/html/rfc6749#section-3.2\" target=\"_blank\">RFC 6749</a>, section 3.2",
              "propertyOrder" : 700,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            },
            "clientId" : {
              "title" : "Client Id",
              "description" : "OAuth client_id parameter<br><br>For more information on the OAuth
 client_id parameter refer to the <a href=\"http://tools.ietf.org/html/rfc6749#section-2.3.1\" target=
\"_blank\">RFC 6749</a>, section 2.3.1",
              "propertyOrder" : 400,
              "required" : true,
              "type" : "string",
```

```
              "exampleValue" : ""
            },
            "ssoProxyUrl" : {
              "title" : "Proxy URL",
              "description" : "The URL to the OpenAM OAuth proxy JSP<br><br>This URL should only be
changed from the default, if an external server is performing the GET to POST proxying. The default
is <code>/openam/oauth2c/OAuthProxy.jsp</code>",
              "propertyOrder" : 1300,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            },
            "usesBasicAuth" : {
              "title" : "Use Basic Auth",
              "description" : "When enabled, the client will use basic auth for authenticating with
the social auth provider. Enabled by default.",
              "propertyOrder" : 1200,
              "required" : true,
              "type" : "boolean",
              "exampleValue" : ""
            },
            "scope" : {
              "title" : "Scope",
              "description" : "OAuth scope; list of user profile properties<br><br>According to the
OAuth 2.0 Authorization Framework, scope is a space-separated list of user profile attributes that
the client application requires. The list depends on the permissions that the resource owner grants
to the client application.<br/><br/> Some authorization servers use non-standard separators for
scopes. For example, Facebook takes a comma-separated list.<br/><br/>",
              "propertyOrder" : 900,
              "required" : true,
              "items" : {
                "type" : "string"
              },
              "type" : "array",
              "exampleValue" : ""
            },
            "subjectProperty" : {
              "title" : "Subject Property",
              "description" : "Property used to identify which attribute an auth server identifies a
user by.",
              "propertyOrder" : 1100,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            },
            "clientSecret" : {
              "title" : "Client Secret",
              "description" : "OAuth client_secret parameter<br><br>For more information on the OAuth
client_secret parameter refer to the <a href=\"http://tools.ietf.org/html/rfc6749#section-2.3.1\"
target=\"_blank\">RFC 6749</a>, section 2.3.1",
              "propertyOrder" : 500,
              "required" : true,
              "type" : "string",
              "format" : "password",
              "exampleValue" : ""
            },
            "scopeDelimiter" : {
              "title" : "Scope Delimiter",
              "description" : "Delimiter used to separate scope values. Default value is space.",
```

```
              "propertyOrder" : 1000,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            },
            "provider" : {
              "title" : "Social Provider",
              "description" : "Social Provider for which this module is being setup.",
              "propertyOrder" : 200,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            },
            "authorizeEndpoint" : {
              "title" : "Authentication Endpoint URL",
              "description" : "OAuth authentication endpoint URL<br><br>This is the URL endpoint for
 OAuth authentication provided by the OAuth Identity Provider",
              "propertyOrder" : 600,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            },
            "authenticationLevel" : {
              "title" : "Authentication Level",
              "description" : "The authentication level associated with this module.<br><br>Each
 authentication module has an authentication level that can be used to indicate the level of security
 associated with the module; 0 is the lowest (and the default).",
              "propertyOrder" : 100,
              "required" : true,
              "type" : "integer",
              "exampleValue" : ""
            },
            "userInfoEndpoint" : {
              "title" : "User Profile Service URL",
              "description" : "User profile information URL<br><br>This URL endpoint provides user
 profile information and is provided by the OAuth Identity Provider<br/><br/><i>NB </i>This URL should
 return JSON objects in response",
              "propertyOrder" : 800,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            }
          }
        }
      },
      "type" : "object",
      "title" : "Realm Defaults"
    }
  }
}
```

SocialAuthentication

Realm Operations

Resource path: `/realm-config/services/socialauthentication`

Resource version: `1.0`

create

Usage:

```
am> create SocialAuthentication --realm Realm --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "displayNames" : {
      "title" : "Display Names",
      "description" : "The display names for the implementations - this will be used to provide a name
 for the icon displayed on the login page. The key should be used across all the settings on this page
 to join them together.<br><br>For example:<table><tr><th>Key</th><th>Value</th></tr><tr><td>google</
td><td>Google</td></tr></table>",
      "propertyOrder" : 100,
      "required" : false,
      "patternProperties" : {
        ".*" : {
          "type" : "string"
        }
      },
      "type" : "object",
      "exampleValue" : ""
    },
    "authenticationChains" : {
      "title" : "Authentication Chains",
      "description" : "The name of the authentication chains that are the entry points to being
 authenticated by each respective social authentication provider. The key should correspond to a
 key used to define a Display Name above.<br><br>For example:<table><tr><th>Key</th><th>Value</th></
tr><tr><td>google</td><td>socialAuthChainGoogle</td></tr></table>",
      "propertyOrder" : 200,
      "required" : false,
      "patternProperties" : {
        ".*" : { }
      },
      "type" : "object",
      "exampleValue" : ""
    },
```

```
    "enabledKeys" : {
      "title" : "Enabled Implementations",
      "description" : "Provide a key that has been used to define the settings above to enable that
 set of settings.<br><br>For example: google",
      "propertyOrder" : 400,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "icons" : {
      "title" : "Icons",
      "description" : "Either a full URL or a path relative to the base of the site/server where the
 image can be found. The image will be used on the login page to link to the authentication chain
 defined above. The key should correspond to a key used to define a Display Name above.<br><br>For
 example:<table><tr><th>Key</th><th>Value</th></tr><tr><td>google</td><td>/images/google-sign-in.png</
td></tr></table>",
      "propertyOrder" : 300,
      "required" : false,
      "patternProperties" : {
        ".*" : {
          "type" : "string"
        }
      },
      "type" : "object",
      "exampleValue" : ""
    }
  }
}
```


delete

Usage:

```
am> delete SocialAuthentication --realm Realm
```

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action SocialAuthentication --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action SocialAuthentication --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action SocialAuthentication --realm Realm --actionName nextdescendents
```

read

Usage:

```
am> read SocialAuthentication --realm Realm
```

update

Usage:

```
am> update SocialAuthentication --realm Realm --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "displayNames" : {
      "title" : "Display Names",
      "description" : "The display names for the implementations - this will be used to provide a name
 for the icon displayed on the login page. The key should be used across all the settings on this page
 to join them together.<br><br>For example:<table><tr><th>Key</th><th>Value</th></tr><tr><td>google</
td><td>Google</td></tr></table>",
      "propertyOrder" : 100,
      "required" : false,
      "patternProperties" : {
        ".*" : {
          "type" : "string"
        }
      },
      "type" : "object",
      "exampleValue" : ""
    },
    "authenticationChains" : {
      "title" : "Authentication Chains",
      "description" : "The name of the authentication chains that are the entry points to being
 authenticated by each respective social authentication provider. The key should correspond to a
 key used to define a Display Name above.<br><br>For example:<table><tr><th>Key</th><th>Value</th></
tr><tr><td>google</td><td>socialAuthChainGoogle</td></tr></table>",
```

```
      "propertyOrder" : 200,
      "required" : false,
      "patternProperties" : {
        ".*" : { }
      },
      "type" : "object",
      "exampleValue" : ""
    },
    "enabledKeys" : {
      "title" : "Enabled Implementations",
      "description" : "Provide a key that has been used to define the settings above to enable that
 set of settings.<br><br>For example: google",
      "propertyOrder" : 400,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "icons" : {
      "title" : "Icons",
      "description" : "Either a full URL or a path relative to the base of the site/server where the
 image can be found. The image will be used on the login page to link to the authentication chain
 defined above. The key should correspond to a key used to define a Display Name above.<br><br>For
 example:<table><tr><th>Key</th><th>Value</th></tr><tr><td>google</td><td>/images/google-sign-in.png</
td></tr></table>",
      "propertyOrder" : 300,
      "required" : false,
      "patternProperties" : {
        ".*" : {
          "type" : "string"
        }
      },
      "type" : "object",
      "exampleValue" : ""
    }
  }
}
```

Global Operations

Resource path: `/global-config/services/socialauthentication`

Resource version: `1.0`

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action SocialAuthentication --global --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action SocialAuthentication --global --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action SocialAuthentication --global --actionName nextdescendents
```

read

Usage:

```
am> read SocialAuthentication --global
```

update

Usage:

```
am> update SocialAuthentication --global --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "defaults" : {
      "properties" : {
        "enabledKeys" : {
          "title" : "Enabled Implementations",
          "description" : "Provide a key that has been used to define the settings above to enable
 that set of settings.<br><br>For example: google",
          "propertyOrder" : 400,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "displayNames" : {
          "title" : "Display Names",
```

```
          "description" : "The display names for the implementations - this will be used to provide
 a name for the icon displayed on the login page. The key should be used across all the settings
 on this page to join them together.<br><br>For example:<table><tr><th>Key</th><th>Value</th></
tr><tr><td>google</td><td>Google</td></tr></table>",
          "propertyOrder" : 100,
          "required" : false,
          "patternProperties" : {
            ".*" : {
              "type" : "string"
            }
          },
          "type" : "object",
          "exampleValue" : ""
        },
        "icons" : {
          "title" : "Icons",
          "description" : "Either a full URL or a path relative to the base of the site/server where
 the image can be found. The image will be used on the login page to link to the authentication chain
 defined above. The key should correspond to a key used to define a Display Name above.<br><br>For
 example:<table><tr><th>Key</th><th>Value</th></tr><tr><td>google</td><td>/images/google-sign-in.png</
td></tr></table>",
          "propertyOrder" : 300,
          "required" : false,
          "patternProperties" : {
            ".*" : {
              "type" : "string"
            }
          },
          "type" : "object",
          "exampleValue" : ""
        },
        "authenticationChains" : {
          "title" : "Authentication Chains",
          "description" : "The name of the authentication chains that are the entry points to being
 authenticated by each respective social authentication provider. The key should correspond to a
 key used to define a Display Name above.<br><br>For example:<table><tr><th>Key</th><th>Value</th></
tr><tr><td>google</td><td>socialAuthChainGoogle</td></tr></table>",
          "propertyOrder" : 200,
          "required" : false,
          "patternProperties" : {
            ".*" : { }
          },
          "type" : "object",
          "exampleValue" : ""
        }
      },
      "type" : "object",
      "title" : "Realm Defaults"
    }
  }
}
```

SocialFacebook

Realm Operations

Resource path: `/realm-config/authentication/authenticationtrees/nodes/SocialFacebookNode`

Resource version: `1.0`

create

Usage:

```
am> create SocialFacebook --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "cfgAttributeMappingConfiguration" : {
      "title" : "Attribute Mapper Configuration",
      "description" : "Mapping of OAuth attributes to local OpenAM attributes Attribute configuration
 that will be used to map the user info obtained from the OAuth 2.0 Provider to the local user data
 store in the OpenAM. Example: OAuth2.0_attribute=local_attribute",
      "propertyOrder" : 1500,
      "patternProperties" : {
        ".*" : {
          "type" : "string"
        }
      },
      "type" : "object",
      "exampleValue" : ""
    },
    "issuer" : {
      "title" : "Token Issuer",
      "description" : "Required when the 'openid' scope is included. Value must match the iss field
 in issued ID Token e.g. accounts.google.com The issuer value MUST be provided when OAuth 2.0 Mix-Up
 Mitigation is enabled.",
      "propertyOrder" : 1800,
      "type" : "string",
      "exampleValue" : ""
    },
    "tokenEndpoint" : {
      "title" : "Access Token Endpoint URL",
```

```
      "description" : "OAuth access token endpoint URL This is the URL endpoint for access token
 retrieval provided by the OAuth Identity Provider.Refer to the RFC 6749 (http://tools.ietf.org/html/
rfc6749#section-3.2), section 3.2.",
      "propertyOrder" : 400,
      "type" : "string",
      "exampleValue" : ""
    },
    "cfgAccountMapperConfiguration" : {
      "title" : "Account Mapper Configuration",
      "description" : "Mapping of OAuth account to local OpenAM account Attribute configuration that
 will be used to map the account of the user authenticated in the OAuth 2.0 Provider to the local data
 store in the OpenAM. Example: <code>OAuth2.0_attribute=local_attribute</code>",
      "propertyOrder" : 1400,
      "patternProperties" : {
        ".*" : {
          "type" : "string"
        }
      },
      "type" : "object",
      "exampleValue" : ""
    },
    "cfgAccountMapperClass" : {
      "title" : "Account Mapper",
      "description" : "Name of the class implementing the attribute mapping for the
 account search. This class is used by the module to map from the account information
 received from the OAuth Identity Provider into OpenAM. The class must implement the
 <code>org.forgerock.openam.authentication.modules.common.mapping.AttributeMapper</code> interface.
 Provided implementations are:
 <code>org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper
 org.forgerock.openam.authentication.modules.oidc.JwtAttributeMapper</code>(can only be used when
 using the openid scope) String constructor parameters can be provided by appending | separated
 values.",
      "propertyOrder" : 1200,
      "type" : "string",
      "exampleValue" : ""
    },
    "basicAuth" : {
      "title" : "Use Basic Auth",
      "description" : "When enabled, the client will use basic auth for authenticating with the social
 auth provider. Enabled by default.",
      "propertyOrder" : 1000,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "provider" : {
      "title" : "Social Provider",
      "description" : "Social Provider for which this module is being setup.",
      "propertyOrder" : 800,
      "type" : "string",
      "exampleValue" : ""
    },
    "userInfoEndpoint" : {
      "title" : "User Profile Service URL",
      "description" : "User profile information URL <p> This URL endpoint provides user profile
 information and is provided by the OAuth Identity Provider NB This URL should return JSON objects in
 response.",
      "propertyOrder" : 500,
      "type" : "string",
      "exampleValue" : ""
```

```
    },
    "authenticationIdKey" : {
      "title" : "Auth ID Key",
      "description" : "",
      "propertyOrder" : 900,
      "type" : "string",
      "exampleValue" : ""
    },
    "cfgMixUpMitigation" : {
      "title" : "OAuth 2.0 Mix-Up Mitigation Enabled",
      "description" : "Enables OAuth 2.0 mix-up mitigation The authorization server must support
 the OAuth 2.0 Mix-Up Mitigation draft (https://tools.ietf.org/html/draft-ietf-oauth-mix-up-
mitigation-01#section-3.1), otherwise OpenAM will fail to validate responses from the authorization
 server. If only the OAuth 2.0 protocol is utilized, make sure that the accepted issuer value is set
 in the \"Token Issuer\" setting.",
      "propertyOrder" : 1700,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "saveUserAttributesToSession" : {
      "title" : "Save Attributes in the Session",
      "description" : "If this option is enabled, the attributes configured in the attribute mapper
 will be saved into the OpenAM session.",
      "propertyOrder" : 1600,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "clientId" : {
      "title" : "Client ID",
      "description" : "OAuth client_id parameter<p> For more information on the OAuth client_id
 parameter refer to the RFC 6749 (http://tools.ietf.org/html/rfc6749#section-2.3.1), section 2.3.1.",
      "propertyOrder" : 100,
      "type" : "string",
      "exampleValue" : ""
    },
    "scopeString" : {
      "title" : "OAuth Scope",
      "description" : "List of user profile properties<p>According to the OAuth 2.0 Authorization
 Framework, scope is a space-separated list of user profile attributes that the client application
 requires. The list depends on the permissions that the resource owner grants to the client
 application. Some authorization servers use non-standard separators for scopes.",
      "propertyOrder" : 600,
      "type" : "string",
      "exampleValue" : ""
    },
    "clientSecret" : {
      "title" : "Client Secret",
      "description" : "OAuth client_secret parameter <p>For more information on the OAuth client_id
 parameter refer to the RFC 6749 (http://tools.ietf.org/html/rfc6749#section-2.3.1), section 2.3.1.",
      "propertyOrder" : 200,
      "type" : "string",
      "format" : "password",
      "exampleValue" : ""
    },
    "authorizeEndpoint" : {
      "title" : "Authentication Endpoint URL",
      "description" : "OAuth authentication endpoint URL <p> This is the URL endpoint for OAuth
 authentication provided by the OAuth Identity Provider.",
      "propertyOrder" : 300,
```

```
      "type" : "string",
      "exampleValue" : ""
    },
    "cfgAccountProviderClass" : {
      "title" : "Account Provider",
      "description" : "Name of the class implementing the account provider. This class is
 used by the module to find the account from the attributes mapped by the Account Mapper
 <code>org.forgerock.openam.authentication.modules.common.mapping.AccountProvider</code> interface.
 String constructor parameters can be provided by appending | separated values.",
      "propertyOrder" : 1100,
      "type" : "string",
      "exampleValue" : ""
    },
    "cfgAttributeMappingClasses" : {
      "title" : "Attribute Mapper",
      "description" : "Name of the class that implements the attribute
 mapping This class maps the OAuth properties into OpenAM properties. A custom
 attribute mapper can be provided. A custom attribute mapper must implement the
 org.forgerock.openam.authentication.modules.common.mapping.AttributeMapper interface. Provided
 implementations are: org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper
 org.forgerock.openam.authentication.modules.oidc.JwtAttributeMapper (can only be used when using the
 openid scope)",
      "propertyOrder" : 1300,
      "items" : {
        "type" : "string"
      },
      "minItems" : 1,
      "type" : "array",
      "exampleValue" : ""
    },
    "redirectURI" : {
      "title" : "Redirect URL",
      "description" : "",
      "propertyOrder" : 700,
      "type" : "string",
      "exampleValue" : ""
    }
  },
  "required" : [ "scopeString", "cfgAccountMapperConfiguration", "cfgAttributeMappingConfiguration",
 "cfgAccountMapperClass", "redirectURI", "clientSecret", "basicAuth", "authenticationIdKey",
 "issuer", "tokenEndpoint", "provider", "cfgAccountProviderClass", "cfgMixUpMitigation",
 "clientId", "authorizeEndpoint", "saveUserAttributesToSession", "userInfoEndpoint",
 "cfgAttributeMappingClasses" ]
}
```


delete

Usage:

```
am> delete SocialFacebook --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action SocialFacebook --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action SocialFacebook --realm Realm --actionName getCreatableTypes
```

listOutcomes

List the available outcomes for the node type.

Usage:

```
am> action SocialFacebook --realm Realm --body body --actionName listOutcomes
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "title" : "Some configuration of the node. This does not need to be complete against the
 configuration schema."
}
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action SocialFacebook --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query SocialFacebook --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read SocialFacebook --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update SocialFacebook --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "cfgAttributeMappingConfiguration" : {
      "title" : "Attribute Mapper Configuration",
      "description" : "Mapping of OAuth attributes to local OpenAM attributes Attribute configuration
 that will be used to map the user info obtained from the OAuth 2.0 Provider to the local user data
 store in the OpenAM. Example: OAuth2.0_attribute=local_attribute",
      "propertyOrder" : 1500,
      "patternProperties" : {
        ".*" : {
          "type" : "string"
        }
      },
      "type" : "object",
      "exampleValue" : ""
    },
    "issuer" : {
      "title" : "Token Issuer",
      "description" : "Required when the 'openid' scope is included. Value must match the iss field
 in issued ID Token e.g. accounts.google.com The issuer value MUST be provided when OAuth 2.0 Mix-Up
 Mitigation is enabled.",
```

```
      "propertyOrder" : 1800,
      "type" : "string",
      "exampleValue" : ""
    },
    "tokenEndpoint" : {
      "title" : "Access Token Endpoint URL",
      "description" : "OAuth access token endpoint URL This is the URL endpoint for access token
 retrieval provided by the OAuth Identity Provider.Refer to the RFC 6749 (http://tools.ietf.org/html/
rfc6749#section-3.2), section 3.2.",
      "propertyOrder" : 400,
      "type" : "string",
      "exampleValue" : ""
    },
    "cfgAccountMapperConfiguration" : {
      "title" : "Account Mapper Configuration",
      "description" : "Mapping of OAuth account to local OpenAM account Attribute configuration that
 will be used to map the account of the user authenticated in the OAuth 2.0 Provider to the local data
 store in the OpenAM. Example: <code>OAuth2.0_attribute=local_attribute</code>",
      "propertyOrder" : 1400,
      "patternProperties" : {
        ".*" : {
          "type" : "string"
        }
      },
      "type" : "object",
      "exampleValue" : ""
    },
    "cfgAccountMapperClass" : {
      "title" : "Account Mapper",
      "description" : "Name of the class implementing the attribute mapping for the
 account search. This class is used by the module to map from the account information
 received from the OAuth Identity Provider into OpenAM. The class must implement the
 <code>org.forgerock.openam.authentication.modules.common.mapping.AttributeMapper</code> interface.
 Provided implementations are:
 <code>org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper
 org.forgerock.openam.authentication.modules.oidc.JwtAttributeMapper</code>(can only be used when
 using the openid scope) String constructor parameters can be provided by appending | separated
 values.",
      "propertyOrder" : 1200,
      "type" : "string",
      "exampleValue" : ""
    },
    "basicAuth" : {
      "title" : "Use Basic Auth",
      "description" : "When enabled, the client will use basic auth for authenticating with the social
 auth provider. Enabled by default.",
      "propertyOrder" : 1000,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "provider" : {
      "title" : "Social Provider",
      "description" : "Social Provider for which this module is being setup.",
      "propertyOrder" : 800,
      "type" : "string",
      "exampleValue" : ""
    },
    "userInfoEndpoint" : {
      "title" : "User Profile Service URL",
```

```
      "description" : "User profile information URL <p> This URL endpoint provides user profile
 information and is provided by the OAuth Identity Provider NB This URL should return JSON objects in
 response.",
      "propertyOrder" : 500,
      "type" : "string",
      "exampleValue" : ""
    },
    "authenticationIdKey" : {
      "title" : "Auth ID Key",
      "description" : "",
      "propertyOrder" : 900,
      "type" : "string",
      "exampleValue" : ""
    },
    "cfgMixUpMitigation" : {
      "title" : "OAuth 2.0 Mix-Up Mitigation Enabled",
      "description" : "Enables OAuth 2.0 mix-up mitigation The authorization server must support
 the OAuth 2.0 Mix-Up Mitigation draft (https://tools.ietf.org/html/draft-ietf-oauth-mix-up-
mitigation-01#section-3.1), otherwise OpenAM will fail to validate responses from the authorization
 server. If only the OAuth 2.0 protocol is utilized, make sure that the accepted issuer value is set
 in the \"Token Issuer\" setting.",
      "propertyOrder" : 1700,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "saveUserAttributesToSession" : {
      "title" : "Save Attributes in the Session",
      "description" : "If this option is enabled, the attributes configured in the attribute mapper
 will be saved into the OpenAM session.",
      "propertyOrder" : 1600,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "clientId" : {
      "title" : "Client ID",
      "description" : "OAuth client_id parameter<p> For more information on the OAuth client_id
 parameter refer to the RFC 6749 (http://tools.ietf.org/html/rfc6749#section-2.3.1), section 2.3.1.",
      "propertyOrder" : 100,
      "type" : "string",
      "exampleValue" : ""
    },
    "scopeString" : {
      "title" : "OAuth Scope",
      "description" : "List of user profile properties<p>According to the OAuth 2.0 Authorization
 Framework, scope is a space-separated list of user profile attributes that the client application
 requires. The list depends on the permissions that the resource owner grants to the client
 application. Some authorization servers use non-standard separators for scopes.",
      "propertyOrder" : 600,
      "type" : "string",
      "exampleValue" : ""
    },
    "clientSecret" : {
      "title" : "Client Secret",
      "description" : "OAuth client_secret parameter <p>For more information on the OAuth client_id
 parameter refer to the RFC 6749 (http://tools.ietf.org/html/rfc6749#section-2.3.1), section 2.3.1.",
      "propertyOrder" : 200,
      "type" : "string",
      "format" : "password",
      "exampleValue" : ""
```

```
    },
    "authorizeEndpoint" : {
      "title" : "Authentication Endpoint URL",
      "description" : "OAuth authentication endpoint URL <p> This is the URL endpoint for OAuth
 authentication provided by the OAuth Identity Provider.",
      "propertyOrder" : 300,
      "type" : "string",
      "exampleValue" : ""
    },
    "cfgAccountProviderClass" : {
      "title" : "Account Provider",
      "description" : "Name of the class implementing the account provider. This class is
 used by the module to find the account from the attributes mapped by the Account Mapper
 <code>org.forgerock.openam.authentication.modules.common.mapping.AccountProvider</code> interface.
 String constructor parameters can be provided by appending | separated values.",
      "propertyOrder" : 1100,
      "type" : "string",
      "exampleValue" : ""
    },
    "cfgAttributeMappingClasses" : {
      "title" : "Attribute Mapper",
      "description" : "Name of the class that implements the attribute
 mapping This class maps the OAuth properties into OpenAM properties. A custom
 attribute mapper can be provided. A custom attribute mapper must implement the
 org.forgerock.openam.authentication.modules.common.mapping.AttributeMapper interface. Provided
 implementations are: org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper
 org.forgerock.openam.authentication.modules.oidc.JwtAttributeMapper (can only be used when using the
 openid scope)",
      "propertyOrder" : 1300,
      "items" : {
        "type" : "string"
      },
      "minItems" : 1,
      "type" : "array",
      "exampleValue" : ""
    },
    "redirectURI" : {
      "title" : "Redirect URL",
      "description" : "",
      "propertyOrder" : 700,
      "type" : "string",
      "exampleValue" : ""
    }
  },
  "required" : [ "scopeString", "cfgAccountMapperConfiguration", "cfgAttributeMappingConfiguration",
 "cfgAccountMapperClass", "redirectURI", "clientSecret", "basicAuth", "authenticationIdKey",
 "issuer", "tokenEndpoint", "provider", "cfgAccountProviderClass", "cfgMixUpMitigation",
 "clientId", "authorizeEndpoint", "saveUserAttributesToSession", "userInfoEndpoint",
 "cfgAttributeMappingClasses" ]
}
```

SocialGoogle

Realm Operations

Resource path: `/realm-config/authentication/authenticationtrees/nodes/SocialGoogleNode`

Resource version: `1.0`

create

Usage:

```
am> create SocialGoogle --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "clientId" : {
      "title" : "Client ID",
      "description" : "OAuth client_id parameter<p> For more information on the OAuth client_id
 parameter refer to the RFC 6749 (http://tools.ietf.org/html/rfc6749#section-2.3.1), section 2.3.1.",
      "propertyOrder" : 100,
      "type" : "string",
      "exampleValue" : ""
    },
    "issuer" : {
      "title" : "Token Issuer",
      "description" : "Required when the 'openid' scope is included. Value must match the iss field
 in issued ID Token e.g. accounts.google.com The issuer value MUST be provided when OAuth 2.0 Mix-Up
 Mitigation is enabled.",
      "propertyOrder" : 1800,
      "type" : "string",
      "exampleValue" : ""
    },
    "cfgAccountMapperClass" : {
      "title" : "Account Mapper",
      "description" : "Name of the class implementing the attribute mapping for the
 account search. This class is used by the module to map from the account information
 received from the OAuth Identity Provider into OpenAM. The class must implement the
 <code>org.forgerock.openam.authentication.modules.common.mapping.AttributeMapper</code> interface.
 Provided implementations are:
 <code>org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper
 org.forgerock.openam.authentication.modules.oidc.JwtAttributeMapper</code>(can only be used when
```

```
 using the openid scope) String constructor parameters can be provided by appending | separated
 values.",
      "propertyOrder" : 1200,
      "type" : "string",
      "exampleValue" : ""
    },
    "cfgAccountMapperConfiguration" : {
      "title" : "Account Mapper Configuration",
      "description" : "Mapping of OAuth account to local OpenAM account Attribute configuration that
 will be used to map the account of the user authenticated in the OAuth 2.0 Provider to the local data
 store in the OpenAM. Example: <code>OAuth2.0_attribute=local_attribute</code>",
      "propertyOrder" : 1400,
      "patternProperties" : {
        ".*" : {
          "type" : "string"
        }
      },
      "type" : "object",
      "exampleValue" : ""
    },
    "saveUserAttributesToSession" : {
      "title" : "Save Attributes in the Session",
      "description" : "If this option is enabled, the attributes configured in the attribute mapper
 will be saved into the OpenAM session.",
      "propertyOrder" : 1600,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "cfgAttributeMappingConfiguration" : {
      "title" : "Attribute Mapper Configuration",
      "description" : "Mapping of OAuth attributes to local OpenAM attributes Attribute configuration
 that will be used to map the user info obtained from the OAuth 2.0 Provider to the local user data
 store in the OpenAM. Example: OAuth2.0_attribute=local_attribute",
      "propertyOrder" : 1500,
      "patternProperties" : {
        ".*" : {
          "type" : "string"
        }
      },
      "type" : "object",
      "exampleValue" : ""
    },
    "basicAuth" : {
      "title" : "Use Basic Auth",
      "description" : "When enabled, the client will use basic auth for authenticating with the social
 auth provider. Enabled by default.",
      "propertyOrder" : 1000,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "cfgMixUpMitigation" : {
      "title" : "OAuth 2.0 Mix-Up Mitigation Enabled",
      "description" : "Enables OAuth 2.0 mix-up mitigation The authorization server must support
 the OAuth 2.0 Mix-Up Mitigation draft (https://tools.ietf.org/html/draft-ietf-oauth-mix-up-
mitigation-01#section-3.1), otherwise OpenAM will fail to validate responses from the authorization
 server. If only the OAuth 2.0 protocol is utilized, make sure that the accepted issuer value is set
 in the \"Token Issuer\" setting.",
      "propertyOrder" : 1700,
      "type" : "boolean",
```

```
      "exampleValue" : ""
    },
    "authorizeEndpoint" : {
      "title" : "Authentication Endpoint URL",
      "description" : "OAuth authentication endpoint URL <p> This is the URL endpoint for OAuth
 authentication provided by the OAuth Identity Provider.",
      "propertyOrder" : 300,
      "type" : "string",
      "exampleValue" : ""
    },
    "tokenEndpoint" : {
      "title" : "Access Token Endpoint URL",
      "description" : "OAuth access token endpoint URL This is the URL endpoint for access token
 retrieval provided by the OAuth Identity Provider.Refer to the RFC 6749 (http://tools.ietf.org/html/
rfc6749#section-3.2), section 3.2.",
      "propertyOrder" : 400,
      "type" : "string",
      "exampleValue" : ""
    },
    "provider" : {
      "title" : "Social Provider",
      "description" : "Social Provider for which this module is being setup.",
      "propertyOrder" : 800,
      "type" : "string",
      "exampleValue" : ""
    },
    "authenticationIdKey" : {
      "title" : "Auth ID Key",
      "description" : "",
      "propertyOrder" : 900,
      "type" : "string",
      "exampleValue" : ""
    },
    "redirectURI" : {
      "title" : "Redirect URL",
      "description" : "",
      "propertyOrder" : 700,
      "type" : "string",
      "exampleValue" : ""
    },
    "cfgAccountProviderClass" : {
      "title" : "Account Provider",
      "description" : "Name of the class implementing the account provider. This class is
 used by the module to find the account from the attributes mapped by the Account Mapper
 <code>org.forgerock.openam.authentication.modules.common.mapping.AccountProvider</code> interface.
 String constructor parameters can be provided by appending | separated values.",
      "propertyOrder" : 1100,
      "type" : "string",
      "exampleValue" : ""
    },
    "userInfoEndpoint" : {
      "title" : "User Profile Service URL",
      "description" : "User profile information URL <p> This URL endpoint provides user profile
 information and is provided by the OAuth Identity Provider NB This URL should return JSON objects in
 response.",
      "propertyOrder" : 500,
      "type" : "string",
      "exampleValue" : ""
    },
```

```
    "scopeString" : {
      "title" : "OAuth Scope",
      "description" : "List of user profile properties<p>According to the OAuth 2.0 Authorization
 Framework, scope is a space-separated list of user profile attributes that the client application
 requires. The list depends on the permissions that the resource owner grants to the client
 application. Some authorization servers use non-standard separators for scopes.",
      "propertyOrder" : 600,
      "type" : "string",
      "exampleValue" : ""
    },
    "cfgAttributeMappingClasses" : {
      "title" : "Attribute Mapper",
      "description" : "Name of the class that implements the attribute
 mapping This class maps the OAuth properties into OpenAM properties. A custom
 attribute mapper can be provided. A custom attribute mapper must implement the
 org.forgerock.openam.authentication.modules.common.mapping.AttributeMapper interface. Provided
 implementations are: org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper
 org.forgerock.openam.authentication.modules.oidc.JwtAttributeMapper (can only be used when using the
 openid scope)",
      "propertyOrder" : 1300,
      "items" : {
        "type" : "string"
      },
      "minItems" : 1,
      "type" : "array",
      "exampleValue" : ""
    },
    "clientSecret" : {
      "title" : "Client Secret",
      "description" : "OAuth client_secret parameter <p>For more information on the OAuth client_id
 parameter refer to the RFC 6749 (http://tools.ietf.org/html/rfc6749#section-2.3.1), section 2.3.1.",
      "propertyOrder" : 200,
      "type" : "string",
      "format" : "password",
      "exampleValue" : ""
    }
  },
  "required" : [ "cfgAttributeMappingConfiguration", "cfgAccountMapperClass", "clientId",
 "scopeString", "cfgAttributeMappingClasses", "provider", "cfgAccountProviderClass", "tokenEndpoint",
 "issuer", "authorizeEndpoint", "userInfoEndpoint", "saveUserAttributesToSession", "redirectURI",
 "clientSecret", "authenticationIdKey", "basicAuth", "cfgAccountMapperConfiguration",
 "cfgMixUpMitigation" ]
}
```


delete

Usage:

```
am> delete SocialGoogle --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action SocialGoogle --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action SocialGoogle --realm Realm --actionName getCreatableTypes
```

listOutcomes

List the available outcomes for the node type.

Usage:

```
am> action SocialGoogle --realm Realm --body body --actionName listOutcomes
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "title" : "Some configuration of the node. This does not need to be complete against the
 configuration schema."
}
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action SocialGoogle --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query SocialGoogle --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read SocialGoogle --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update SocialGoogle --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "clientId" : {
      "title" : "Client ID",
      "description" : "OAuth client_id parameter<p> For more information on the OAuth client_id
 parameter refer to the RFC 6749 (http://tools.ietf.org/html/rfc6749#section-2.3.1), section 2.3.1.",
      "propertyOrder" : 100,
      "type" : "string",
      "exampleValue" : ""
    },
    "issuer" : {
      "title" : "Token Issuer",
      "description" : "Required when the 'openid' scope is included. Value must match the iss field
 in issued ID Token e.g. accounts.google.com The issuer value MUST be provided when OAuth 2.0 Mix-Up
 Mitigation is enabled.",
      "propertyOrder" : 1800,
      "type" : "string",
      "exampleValue" : ""
    },
    "cfgAccountMapperClass" : {
      "title" : "Account Mapper",
```

```
     "description" : "Name of the class implementing the attribute mapping for the
account search. This class is used by the module to map from the account information
received from the OAuth Identity Provider into OpenAM. The class must implement the
<code>org.forgerock.openam.authentication.modules.common.mapping.AttributeMapper</code> interface.
Provided implementations are:
<code>org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper
org.forgerock.openam.authentication.modules.oidc.JwtAttributeMapper</code>(can only be used when
using the openid scope) String constructor parameters can be provided by appending | separated
values.",
     "propertyOrder" : 1200,
     "type" : "string",
     "exampleValue" : ""
   },
   "cfgAccountMapperConfiguration" : {
     "title" : "Account Mapper Configuration",
     "description" : "Mapping of OAuth account to local OpenAM account Attribute configuration that
will be used to map the account of the user authenticated in the OAuth 2.0 Provider to the local data
store in the OpenAM. Example: <code>OAuth2.0_attribute=local_attribute</code>",
     "propertyOrder" : 1400,
     "patternProperties" : {
       ".*" : {
         "type" : "string"
       }
     },
     "type" : "object",
     "exampleValue" : ""
   },
   "saveUserAttributesToSession" : {
     "title" : "Save Attributes in the Session",
     "description" : "If this option is enabled, the attributes configured in the attribute mapper
will be saved into the OpenAM session.",
     "propertyOrder" : 1600,
     "type" : "boolean",
     "exampleValue" : ""
   },
   "cfgAttributeMappingConfiguration" : {
     "title" : "Attribute Mapper Configuration",
     "description" : "Mapping of OAuth attributes to local OpenAM attributes Attribute configuration
that will be used to map the user info obtained from the OAuth 2.0 Provider to the local user data
store in the OpenAM. Example: OAuth2.0_attribute=local_attribute",
     "propertyOrder" : 1500,
     "patternProperties" : {
       ".*" : {
         "type" : "string"
       }
     },
     "type" : "object",
     "exampleValue" : ""
   },
   "basicAuth" : {
     "title" : "Use Basic Auth",
     "description" : "When enabled, the client will use basic auth for authenticating with the social
auth provider. Enabled by default.",
     "propertyOrder" : 1000,
     "type" : "boolean",
     "exampleValue" : ""
   },
   "cfgMixUpMitigation" : {
     "title" : "OAuth 2.0 Mix-Up Mitigation Enabled",
```

```
      "description" : "Enables OAuth 2.0 mix-up mitigation The authorization server must support
 the OAuth 2.0 Mix-Up Mitigation draft (https://tools.ietf.org/html/draft-ietf-oauth-mix-up-
mitigation-01#section-3.1), otherwise OpenAM will fail to validate responses from the authorization
 server. If only the OAuth 2.0 protocol is utilized, make sure that the accepted issuer value is set
 in the \"Token Issuer\" setting.",
      "propertyOrder" : 1700,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "authorizeEndpoint" : {
      "title" : "Authentication Endpoint URL",
      "description" : "OAuth authentication endpoint URL <p> This is the URL endpoint for OAuth
 authentication provided by the OAuth Identity Provider.",
      "propertyOrder" : 300,
      "type" : "string",
      "exampleValue" : ""
    },
    "tokenEndpoint" : {
      "title" : "Access Token Endpoint URL",
      "description" : "OAuth access token endpoint URL This is the URL endpoint for access token
 retrieval provided by the OAuth Identity Provider.Refer to the RFC 6749 (http://tools.ietf.org/html/
rfc6749#section-3.2), section 3.2.",
      "propertyOrder" : 400,
      "type" : "string",
      "exampleValue" : ""
    },
    "provider" : {
      "title" : "Social Provider",
      "description" : "Social Provider for which this module is being setup.",
      "propertyOrder" : 800,
      "type" : "string",
      "exampleValue" : ""
    },
    "authenticationIdKey" : {
      "title" : "Auth ID Key",
      "description" : "",
      "propertyOrder" : 900,
      "type" : "string",
      "exampleValue" : ""
    },
    "redirectURI" : {
      "title" : "Redirect URL",
      "description" : "",
      "propertyOrder" : 700,
      "type" : "string",
      "exampleValue" : ""
    },
    "cfgAccountProviderClass" : {
      "title" : "Account Provider",
      "description" : "Name of the class implementing the account provider. This class is
 used by the module to find the account from the attributes mapped by the Account Mapper
 <code>org.forgerock.openam.authentication.modules.common.mapping.AccountProvider</code> interface.
 String constructor parameters can be provided by appending | separated values.",
      "propertyOrder" : 1100,
      "type" : "string",
      "exampleValue" : ""
    },
    "userInfoEndpoint" : {
      "title" : "User Profile Service URL",
```

```
      "description" : "User profile information URL <p> This URL endpoint provides user profile
 information and is provided by the OAuth Identity Provider NB This URL should return JSON objects in
 response.",
      "propertyOrder" : 500,
      "type" : "string",
      "exampleValue" : ""
    },
    "scopeString" : {
      "title" : "OAuth Scope",
      "description" : "List of user profile properties<p>According to the OAuth 2.0 Authorization
 Framework, scope is a space-separated list of user profile attributes that the client application
 requires. The list depends on the permissions that the resource owner grants to the client
 application. Some authorization servers use non-standard separators for scopes.",
      "propertyOrder" : 600,
      "type" : "string",
      "exampleValue" : ""
    },
    "cfgAttributeMappingClasses" : {
      "title" : "Attribute Mapper",
      "description" : "Name of the class that implements the attribute
 mapping This class maps the OAuth properties into OpenAM properties. A custom
 attribute mapper can be provided. A custom attribute mapper must implement the
 org.forgerock.openam.authentication.modules.common.mapping.AttributeMapper interface. Provided
 implementations are: org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper
 org.forgerock.openam.authentication.modules.oidc.JwtAttributeMapper (can only be used when using the
 openid scope)",
      "propertyOrder" : 1300,
      "items" : {
        "type" : "string"
      },
      "minItems" : 1,
      "type" : "array",
      "exampleValue" : ""
    },
    "clientSecret" : {
      "title" : "Client Secret",
      "description" : "OAuth client_secret parameter <p>For more information on the OAuth client_id
 parameter refer to the RFC 6749 (http://tools.ietf.org/html/rfc6749#section-2.3.1), section 2.3.1.",
      "propertyOrder" : 200,
      "type" : "string",
      "format" : "password",
      "exampleValue" : ""
    }
  },
  "required" : [ "cfgAttributeMappingConfiguration", "cfgAccountMapperClass", "clientId",
 "scopeString", "cfgAttributeMappingClasses", "provider", "cfgAccountProviderClass", "tokenEndpoint",
 "issuer", "authorizeEndpoint", "userInfoEndpoint", "saveUserAttributesToSession", "redirectURI",
 "clientSecret", "authenticationIdKey", "basicAuth", "cfgAccountMapperConfiguration",
 "cfgMixUpMitigation" ]
}
```

SocialIdentityProviders

Realm Operations

Collection of configured social identity providers.

Resource path: `/selfservice/socialIdentityProviders`

Resource version: `1.0`

read

Reads the list of configured social identity providers.

Usage:

```
am> read SocialIdentityProviders --realm Realm
```

SocialIdentityProvidersConfig

Realm Operations

Resource path: `/realm-config/services/SocialIdentityProviders`

Resource version: `1.0`

create

Usage:

```
am> create SocialIdentityProvidersConfig --realm Realm --body body
```

Parameters:

`--body`

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "enabled" : {
      "title" : "Enabled",
      "description" : "",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    }
  }
}
```

delete

Usage:

```
am> delete SocialIdentityProvidersConfig --realm Realm
```

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action SocialIdentityProvidersConfig --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action SocialIdentityProvidersConfig --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action SocialIdentityProvidersConfig --realm Realm --actionName nextdescendents
```

read

Usage:

```
am> read SocialIdentityProvidersConfig --realm Realm
```

update

Usage:

```
am> update SocialIdentityProvidersConfig --realm Realm --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "enabled" : {
      "title" : "Enabled",
      "description" : "",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    }
  }
}
```

Global Operations

Resource path: `/global-config/services/SocialIdentityProviders`

Resource version: `1.0`

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action SocialIdentityProvidersConfig --global --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action SocialIdentityProvidersConfig --global --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action SocialIdentityProvidersConfig --global --actionName nextdescendents
```

read

Usage:

```
am> read SocialIdentityProvidersConfig --global
```

update

Usage:

```
am> update SocialIdentityProvidersConfig --global --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "defaults" : {
      "properties" : {
        "enabled" : {
          "title" : "Enabled",
          "description" : "",
          "propertyOrder" : 100,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        }
      },
      "type" : "object",
      "title" : "Realm Defaults"
    }
  }
}
```

SocialIgnoreProfile

Realm Operations

Resource path: `/realm-config/authentication/authenticationtrees/nodes/SocialOAuthIgnoreProfileNode`

Resource version: `1.0`

create

Usage:

```
am> create SocialIgnoreProfile --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "required" : [ ]
}
```

delete

Usage:

```
am> delete SocialIgnoreProfile --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action SocialIgnoreProfile --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action SocialIgnoreProfile --realm Realm --actionName getCreatableTypes
```

listOutcomes

List the available outcomes for the node type.

Usage:

```
am> action SocialIgnoreProfile --realm Realm --body body --actionName listOutcomes
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "title" : "Some configuration of the node. This does not need to be complete against the
 configuration schema."
}
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action SocialIgnoreProfile --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query SocialIgnoreProfile --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read SocialIgnoreProfile --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update SocialIgnoreProfile --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "required" : [ ]
}
```

SocialProviderHandlerNode

Realm Operations

Resource path: `/realm-config/authentication/authenticationtrees/nodes/SocialProviderHandlerNode`

Resource version: `1.0`

create

Usage:

```
am> create SocialProviderHandlerNode --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "usernameAttribute" : {
      "title" : "Username Attribute",
      "description" : "The attribute in IDM that contains the username for this object.",
      "propertyOrder" : 300,
      "type" : "string",
      "exampleValue" : ""
    },
    "script" : {
      "title" : "Transformation Script",
      "description" : "A script that can transform a normalized social profile to object data.",
      "propertyOrder" : 100,
      "type" : "string",
      "exampleValue" : ""
    }
  },
  "required" : [ "usernameAttribute", "script" ]
}
```

delete

Usage:

```
am> delete SocialProviderHandlerNode --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action SocialProviderHandlerNode --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action SocialProviderHandlerNode --realm Realm --actionName getCreatableTypes
```

listOutcomes

List the available outcomes for the node type.

Usage:

```
am> action SocialProviderHandlerNode --realm Realm --body body --actionName listOutcomes
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "title" : "Some configuration of the node. This does not need to be complete against the
 configuration schema."
}
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action SocialProviderHandlerNode --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query SocialProviderHandlerNode --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read SocialProviderHandlerNode --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update SocialProviderHandlerNode --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "usernameAttribute" : {
      "title" : "Username Attribute",
      "description" : "The attribute in IDM that contains the username for this object.",
      "propertyOrder" : 300,
      "type" : "string",
      "exampleValue" : ""
    },
    "script" : {
      "title" : "Transformation Script",
      "description" : "A script that can transform a normalized social profile to object data.",
      "propertyOrder" : 100,
      "type" : "string",
      "exampleValue" : ""
    }
  },
  "required" : [ "usernameAttribute", "script" ]
}
```

SoftwarePublisher

Realm Operations

Agents handler that is responsible for managing agents

Resource path: `/realm-config/agents/SoftwarePublisher`

Resource version: `1.0`

create

Usage:

```
am> create SoftwarePublisher --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "jwksUri" : {
      "title" : "Json Web Key URI",
      "description" : "The URI that contains the Software Publisher's public keys in Json Web Key
 format.",
      "propertyOrder" : 34800,
      "type" : "object",
      "exampleValue" : "",
      "properties" : {
        "inherited" : {
          "type" : "boolean",
          "required" : true
        },
        "value" : {
          "type" : "string",
          "required" : false
        }
      }
    },
    "issuer" : {
      "title" : "Software publisher issuer",
      "description" : "Identifier for the software publisher, generally represented as a URL.",
      "propertyOrder" : 33001,
      "type" : "object",
      "exampleValue" : "",
      "properties" : {
        "inherited" : {
          "type" : "boolean",
          "required" : true
        },
        "value" : {
          "type" : "string",
          "required" : true
        }
      }
    },
    "userpassword" : {
      "title" : "Software publisher secret",
      "description" : "Software publisher secret. Used when software statement signatures are HMAC
 based.",
      "propertyOrder" : 33000,
      "required" : true,
      "type" : "string",
      "format" : "password",
```

```
      "exampleValue" : ""
    },
    "softwareStatementSigningAlgorithm" : {
      "title" : "Software statement signing Algorithm",
      "description" : "Signing algorithm to be used when verifying software statement signatures.",
      "propertyOrder" : 34500,
      "type" : "object",
      "exampleValue" : "",
      "properties" : {
        "inherited" : {
          "type" : "boolean",
          "required" : true
        },
        "value" : {
          "type" : "string",
          "required" : false
        }
      }
    },
    "publicKeyLocation" : {
      "title" : "Public key selector",
      "description" : "Select how the Software Publisher's public keys should be retrieved by the
provider when validating software statement signatures.",
      "propertyOrder" : 34700,
      "type" : "object",
      "exampleValue" : "",
      "properties" : {
        "inherited" : {
          "type" : "boolean",
          "required" : true
        },
        "value" : {
          "type" : "string",
          "required" : false
        }
      }
    },
    "jwkSet" : {
      "title" : "Json Web Key",
      "description" : "Raw JSON Web Key value containing the Software Publisher's public keys.",
      "propertyOrder" : 35100,
      "type" : "object",
      "exampleValue" : "",
      "properties" : {
        "inherited" : {
          "type" : "boolean",
          "required" : true
        },
        "value" : {
          "type" : "string",
          "required" : false
        }
      }
    },
    "jwksCacheTimeout" : {
      "title" : "JWKs URI content cache timeout in ms",
      "description" : "To avoid loading the JWKS URI content for every operation, the JWKS content is
cached. This timeout defines the maximum amount of time the JWKS URI content can be cached before
being refreshed.",
```

```
      "propertyOrder" : 34900,
      "type" : "object",
      "exampleValue" : "",
      "properties" : {
        "inherited" : {
          "type" : "boolean",
          "required" : true
        },
        "value" : {
          "type" : "integer",
          "required" : false
        }
      }
    },
    "jwkStoreCacheMissCacheTime" : {
      "title" : "JWKs URI content cache miss cache time",
      "description" : "To avoid loading the JWKS URI content for every operation, especially when
 the kid is not in the jwks content already cached, the JWKS content will be cached for a minimum
 period of time. This cache miss cache time defines the minimum amount of time the JWKS URI content is
 cached.",
      "propertyOrder" : 35000,
      "type" : "object",
      "exampleValue" : "",
      "properties" : {
        "inherited" : {
          "type" : "boolean",
          "required" : true
        },
        "value" : {
          "type" : "integer",
          "required" : false
        }
      }
    },
    "agentgroup" : {
      "title" : "Group",
      "description" : "Add the agent to a group to allow inheritance of property values from the
 group. <br>Changing the group will update inherited property values. <br>Inherited property values
 are copied to the agent.",
      "propertyOrder" : 50,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
```

delete

Usage:

```
am> delete SoftwarePublisher --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action SoftwarePublisher --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action SoftwarePublisher --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action SoftwarePublisher --realm Realm --actionName nextdescendents
```

query

Querying the agents of a specific type

Usage:

```
am> query SoftwarePublisher --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read SoftwarePublisher --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update SoftwarePublisher --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "jwksUri" : {
      "title" : "Json Web Key URI",
      "description" : "The URI that contains the Software Publisher's public keys in Json Web Key
 format.",
      "propertyOrder" : 34800,
      "type" : "object",
      "exampleValue" : "",
      "properties" : {
        "inherited" : {
          "type" : "boolean",
          "required" : true
        },
        "value" : {
          "type" : "string",
          "required" : false
        }
      }
    },
    "issuer" : {
      "title" : "Software publisher issuer",
      "description" : "Identifier for the software publisher, generally represented as a URL.",
      "propertyOrder" : 33001,
      "type" : "object",
      "exampleValue" : "",
      "properties" : {
        "inherited" : {
          "type" : "boolean",
          "required" : true
        },
        "value" : {
          "type" : "string",
          "required" : true
        }
```

```
      }
    },
    "userpassword" : {
      "title" : "Software publisher secret",
      "description" : "Software publisher secret. Used when software statement signatures are HMAC
based.",
      "propertyOrder" : 33000,
      "required" : true,
      "type" : "string",
      "format" : "password",
      "exampleValue" : ""
    },
    "softwareStatementSigningAlgorithm" : {
      "title" : "Software statement signing Algorithm",
      "description" : "Signing algorithm to be used when verifying software statement signatures.",
      "propertyOrder" : 34500,
      "type" : "object",
      "exampleValue" : "",
      "properties" : {
        "inherited" : {
          "type" : "boolean",
          "required" : true
        },
        "value" : {
          "type" : "string",
          "required" : false
        }
      }
    },
    "publicKeyLocation" : {
      "title" : "Public key selector",
      "description" : "Select how the Software Publisher's public keys should be retrieved by the
provider when validating software statement signatures.",
      "propertyOrder" : 34700,
      "type" : "object",
      "exampleValue" : "",
      "properties" : {
        "inherited" : {
          "type" : "boolean",
          "required" : true
        },
        "value" : {
          "type" : "string",
          "required" : false
        }
      }
    },
    "jwkSet" : {
      "title" : "Json Web Key",
      "description" : "Raw JSON Web Key value containing the Software Publisher's public keys.",
      "propertyOrder" : 35100,
      "type" : "object",
      "exampleValue" : "",
      "properties" : {
        "inherited" : {
          "type" : "boolean",
          "required" : true
        },
        "value" : {
```

```
          "type" : "string",
          "required" : false
        }
      }
    },
    "jwksCacheTimeout" : {
      "title" : "JWKs URI content cache timeout in ms",
      "description" : "To avoid loading the JWKS URI content for every operation, the JWKS content is
 cached. This timeout defines the maximum amount of time the JWKS URI content can be cached before
 being refreshed.",
      "propertyOrder" : 34900,
      "type" : "object",
      "exampleValue" : "",
      "properties" : {
        "inherited" : {
          "type" : "boolean",
          "required" : true
        },
        "value" : {
          "type" : "integer",
          "required" : false
        }
      }
    },
    "jwkStoreCacheMissCacheTime" : {
      "title" : "JWKs URI content cache miss cache time",
      "description" : "To avoid loading the JWKS URI content for every operation, especially when
 the kid is not in the jwks content already cached, the JWKS content will be cached for a minimum
 period of time. This cache miss cache time defines the minimum amount of time the JWKS URI content is
 cached.",
      "propertyOrder" : 35000,
      "type" : "object",
      "exampleValue" : "",
      "properties" : {
        "inherited" : {
          "type" : "boolean",
          "required" : true
        },
        "value" : {
          "type" : "integer",
          "required" : false
        }
      }
    },
    "agentgroup" : {
      "title" : "Group",
      "description" : "Add the agent to a group to allow inheritance of property values from the
 group. <br>Changing the group will update inherited property values. <br>Inherited property values
 are copied to the agent.",
      "propertyOrder" : 50,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
```

Splunk

Realm Operations

Resource path: `/realm-config/services/audit/Splunk`

Resource version: `1.0`

create

Usage:

```
am> create Splunk --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "commonHandler" : {
      "type" : "object",
      "title" : "General Handler Configuration",
      "propertyOrder" : 0,
      "properties" : {
        "topics" : {
          "title" : "Topics",
          "description" : "List of topics handled by an audit event handler.",
          "propertyOrder" : 200,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "enabled" : {
          "title" : "Enabled",
          "description" : "Enables or disables an audit event handler.",
          "propertyOrder" : 100,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        }
      }
    },
```

```
   "splunkBuffering" : {
     "type" : "object",
     "title" : "Buffering",
     "propertyOrder" : 3,
     "properties" : {
       "maxEvents" : {
         "title" : "Queue Capacity",
         "description" : "Maximum number of audit evens in the batch queue; additional events are
dropped.",
         "propertyOrder" : 700,
         "required" : true,
         "type" : "integer",
         "exampleValue" : ""
       },
       "writeInterval" : {
         "title" : "Write interval (in milliseconds)",
         "description" : "Interval at which buffered events are written to Splunk.",
         "propertyOrder" : 800,
         "required" : true,
         "type" : "integer",
         "exampleValue" : ""
       },
       "batchSize" : {
         "title" : "Batch Size",
         "description" : "Maximum number of events that can be buffered (default: 10000).",
         "propertyOrder" : 600,
         "required" : true,
         "type" : "integer",
         "exampleValue" : ""
       }
     }
   },
   "splunkConfig" : {
     "type" : "object",
     "title" : "Splunk Configuration",
     "propertyOrder" : 2,
     "properties" : {
       "authzToken" : {
         "title" : "Authorization Token",
         "description" : "Authorization token used to connect to Splunk HTTP Event Collector
endpoint.",
         "propertyOrder" : null,
         "required" : true,
         "type" : "string",
         "exampleValue" : ""
       },
       "host" : {
         "title" : "Server Hostname",
         "description" : "Host name or IP address of Splunk server.",
         "propertyOrder" : 300,
         "required" : true,
         "type" : "string",
         "exampleValue" : ""
       },
       "sslEnabled" : {
         "title" : "SSL Enabled",
         "description" : "Use HTTPS protocol for communication with Splunk.",
         "propertyOrder" : 500,
         "required" : true,
```

```
          "type" : "boolean",
          "exampleValue" : ""
        },
        "port" : {
          "title" : "Server Port",
          "description" : "Port number of Splunk server.",
          "propertyOrder" : 400,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        }
      }
    },
    "commonHandlerPlugin" : {
      "type" : "object",
      "title" : "Audit Event Handler Factory",
      "propertyOrder" : 1,
      "properties" : {
        "handlerFactory" : {
          "title" : "Factory Class Name",
          "description" : "The fully qualified class name of the factory
 responsible for creating the Audit Event Handler. The class must implement
 <code>org.forgerock.openam.audit.AuditEventHandlerFactory</code>.",
          "propertyOrder" : null,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    }
  }
}
```

delete

Usage:

```
am> delete Splunk --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action Splunk --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action Splunk --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action Splunk --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query Splunk --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read Splunk --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update Splunk --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "commonHandler" : {
      "type" : "object",
      "title" : "General Handler Configuration",
      "propertyOrder" : 0,
      "properties" : {
        "topics" : {
          "title" : "Topics",
          "description" : "List of topics handled by an audit event handler.",
          "propertyOrder" : 200,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "enabled" : {
          "title" : "Enabled",
          "description" : "Enables or disables an audit event handler.",
          "propertyOrder" : 100,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        }
      }
    },
    "splunkBuffering" : {
      "type" : "object",
      "title" : "Buffering",
      "propertyOrder" : 3,
      "properties" : {
        "maxEvents" : {
          "title" : "Queue Capacity",
          "description" : "Maximum number of audit evens in the batch queue; additional events are
 dropped.",
          "propertyOrder" : 700,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "writeInterval" : {
          "title" : "Write interval (in milliseconds)",
          "description" : "Interval at which buffered events are written to Splunk.",
          "propertyOrder" : 800,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
```

```
        "batchSize" : {
          "title" : "Batch Size",
          "description" : "Maximum number of events that can be buffered (default: 10000).",
          "propertyOrder" : 600,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        }
      }
    },
    "splunkConfig" : {
      "type" : "object",
      "title" : "Splunk Configuration",
      "propertyOrder" : 2,
      "properties" : {
        "authzToken" : {
          "title" : "Authorization Token",
          "description" : "Authorization token used to connect to Splunk HTTP Event Collector
endpoint.",
          "propertyOrder" : null,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "host" : {
          "title" : "Server Hostname",
          "description" : "Host name or IP address of Splunk server.",
          "propertyOrder" : 300,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "sslEnabled" : {
          "title" : "SSL Enabled",
          "description" : "Use HTTPS protocol for communication with Splunk.",
          "propertyOrder" : 500,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "port" : {
          "title" : "Server Port",
          "description" : "Port number of Splunk server.",
          "propertyOrder" : 400,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        }
      }
    },
    "commonHandlerPlugin" : {
      "type" : "object",
      "title" : "Audit Event Handler Factory",
      "propertyOrder" : 1,
      "properties" : {
        "handlerFactory" : {
          "title" : "Factory Class Name",
```

```
          "description" : "The fully qualified class name of the factory
 responsible for creating the Audit Event Handler. The class must implement
 <code>org.forgerock.openam.audit.AuditEventHandlerFactory</code>.",
          "propertyOrder" : null,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    }
  }
}
```

Global Operations

Resource path: `/global-config/services/audit/Splunk`

Resource version: `1.0`

create

Usage:

```
am> create Splunk --global --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "splunkConfig" : {
      "type" : "object",
      "title" : "Splunk Configuration",
      "propertyOrder" : 2,
      "properties" : {
        "host" : {
          "title" : "Server Hostname",
          "description" : "Host name or IP address of Splunk server.",
          "propertyOrder" : 300,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "sslEnabled" : {
          "title" : "SSL Enabled",
          "description" : "Use HTTPS protocol for communication with Splunk.",
```

```
          "propertyOrder" : 500,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "authzToken" : {
          "title" : "Authorization Token",
          "description" : "Authorization token used to connect to Splunk HTTP Event Collector
endpoint.",
          "propertyOrder" : null,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "port" : {
          "title" : "Server Port",
          "description" : "Port number of Splunk server.",
          "propertyOrder" : 400,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        }
      }
    },
    "commonHandler" : {
      "type" : "object",
      "title" : "General Handler Configuration",
      "propertyOrder" : 0,
      "properties" : {
        "topics" : {
          "title" : "Topics",
          "description" : "List of topics handled by an audit event handler.",
          "propertyOrder" : 200,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "enabled" : {
          "title" : "Enabled",
          "description" : "Enables or disables an audit event handler.",
          "propertyOrder" : 100,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        }
      }
    },
    "splunkBuffering" : {
      "type" : "object",
      "title" : "Buffering",
      "propertyOrder" : 3,
      "properties" : {
        "maxEvents" : {
          "title" : "Queue Capacity",
          "description" : "Maximum number of audit evens in the batch queue; additional events are
dropped.",
```

```
          "propertyOrder" : 700,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "batchSize" : {
          "title" : "Batch Size",
          "description" : "Maximum number of events that can be buffered (default: 10000).",
          "propertyOrder" : 600,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "writeInterval" : {
          "title" : "Write interval (in milliseconds)",
          "description" : "Interval at which buffered events are written to Splunk.",
          "propertyOrder" : 800,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        }
      }
    },
    "commonHandlerPlugin" : {
      "type" : "object",
      "title" : "Audit Event Handler Factory",
      "propertyOrder" : 1,
      "properties" : {
        "handlerFactory" : {
          "title" : "Factory Class Name",
          "description" : "The fully qualified class name of the factory
 responsible for creating the Audit Event Handler. The class must implement
 <code>org.forgerock.openam.audit.AuditEventHandlerFactory</code>.",
          "propertyOrder" : null,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    }
  }
}
```


delete

Usage:

```
am> delete Splunk --global --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action Splunk --global --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action Splunk --global --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action Splunk --global --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query Splunk --global --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read Splunk --global --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update Splunk --global --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "splunkConfig" : {
      "type" : "object",
      "title" : "Splunk Configuration",
      "propertyOrder" : 2,
      "properties" : {
        "host" : {
          "title" : "Server Hostname",
          "description" : "Host name or IP address of Splunk server.",
          "propertyOrder" : 300,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "sslEnabled" : {
          "title" : "SSL Enabled",
          "description" : "Use HTTPS protocol for communication with Splunk.",
          "propertyOrder" : 500,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "authzToken" : {
          "title" : "Authorization Token",
          "description" : "Authorization token used to connect to Splunk HTTP Event Collector
 endpoint.",
          "propertyOrder" : null,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "port" : {
          "title" : "Server Port",
          "description" : "Port number of Splunk server.",
          "propertyOrder" : 400,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        }
      }
```

```
    },
    "commonHandler" : {
      "type" : "object",
      "title" : "General Handler Configuration",
      "propertyOrder" : 0,
      "properties" : {
        "topics" : {
          "title" : "Topics",
          "description" : "List of topics handled by an audit event handler.",
          "propertyOrder" : 200,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "enabled" : {
          "title" : "Enabled",
          "description" : "Enables or disables an audit event handler.",
          "propertyOrder" : 100,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        }
      }
    },
    "splunkBuffering" : {
      "type" : "object",
      "title" : "Buffering",
      "propertyOrder" : 3,
      "properties" : {
        "maxEvents" : {
          "title" : "Queue Capacity",
          "description" : "Maximum number of audit evens in the batch queue; additional events are
dropped.",
          "propertyOrder" : 700,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "batchSize" : {
          "title" : "Batch Size",
          "description" : "Maximum number of events that can be buffered (default: 10000).",
          "propertyOrder" : 600,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "writeInterval" : {
          "title" : "Write interval (in milliseconds)",
          "description" : "Interval at which buffered events are written to Splunk.",
          "propertyOrder" : 800,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        }
      }
    },
```

```
    "commonHandlerPlugin" : {
      "type" : "object",
      "title" : "Audit Event Handler Factory",
      "propertyOrder" : 1,
      "properties" : {
        "handlerFactory" : {
          "title" : "Factory Class Name",
          "description" : "The fully qualified class name of the factory
 responsible for creating the Audit Event Handler. The class must implement
 <code>org.forgerock.openam.audit.AuditEventHandlerFactory</code>.",
          "propertyOrder" : null,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    }
  }
}
```

StateMetadata

Realm Operations

Resource path: `/realm-config/authentication/authenticationtrees/nodes/MetadataNode`

Resource version: `1.0`

create

Usage:

```
am> create StateMetadata --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "attributes" : {
      "title" : "Attributes",
      "description" : "List of attributes that will be selected from the shared state (if they exist)
 and will be returned to the user-agent in a metadata callback.",
      "propertyOrder" : 100,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    }
  },
  "required" : [ "attributes" ]
}
```

delete

Usage:

```
am> delete StateMetadata --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action StateMetadata --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action StateMetadata --realm Realm --actionName getCreatableTypes
```

listOutcomes

List the available outcomes for the node type.

Usage:

```
am> action StateMetadata --realm Realm --body body --actionName listOutcomes
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "title" : "Some configuration of the node. This does not need to be complete against the
 configuration schema."
}
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action StateMetadata --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query StateMetadata --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read StateMetadata --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update StateMetadata --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "attributes" : {
      "title" : "Attributes",
      "description" : "List of attributes that will be selected from the shared state (if they exist)
 and will be returned to the user-agent in a metadata callback.",
      "propertyOrder" : 100,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    }
  },
  "required" : [ "attributes" ]
}
```

SubjectAttributes

Realm Operations

Service for querying subject attributes stored in OpenAM. When you define a policy subject condition, the condition can depend on values of subject attributes stored in a user's profile. The list of possible subject attributes that you can use depends on the LDAP User Attributes configured for the Identity data store where OpenAM looks up the user's profile

Resource path: `/subjectattributes`

Resource version: `1.0`

query

Query the list of subject attributes stored in OpenAM

Usage:

```
am> query SubjectAttributes --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all. Fields that can be queried: [*]

SubjectTypes

Realm Operations

Service for querying and reading the subject types stored in OpenAM. Subject condition types describe the JSON representation of subject conditions that you can use in policy definitions

Resource path: `/subjecttypes`

Resource version: `1.0`

query

Query the list of subject condition types

Usage:

```
am> query SubjectTypes --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all. Fields that can be queried: [*]

read

Read an individual subject condition type by providing the unique identifier title

Usage:

```
am> read SubjectTypes --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

SuccessURL

Realm Operations

Resource path: `/realm-config/authentication/authenticationtrees/nodes/SetSuccessUrlNode`

Resource version: `1.0`

create

Usage:

```
am> create SuccessURL --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "successUrl" : {
      "title" : "Success URL",
      "description" : "",
      "propertyOrder" : 100,
      "type" : "string",
      "exampleValue" : ""
    }
  },
  "required" : [ "successUrl" ]
}
```

delete

Usage:

```
am> delete SuccessURL --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action SuccessURL --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action SuccessURL --realm Realm --actionName getCreatableTypes
```

listOutcomes

List the available outcomes for the node type.

Usage:

```
am> action SuccessURL --realm Realm --body body --actionName listOutcomes
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "title" : "Some configuration of the node. This does not need to be complete against the
 configuration schema."
}
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action SuccessURL --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query SuccessURL --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read SuccessURL --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update SuccessURL --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "successUrl" : {
      "title" : "Success URL",
      "description" : "",
      "propertyOrder" : 100,
      "type" : "string",
      "exampleValue" : ""
    }
  },
  "required" : [ "successUrl" ]
}
```

SunDSWithOpenAMSchema

Realm Operations

Resource path: `/realm-config/services/id-repositories/LDAPv3ForAMDS`

Resource version: `1.0`

create

Usage:

```
am> create SunDSWithOpenAMSchema --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "roleconfig" : {
      "type" : "object",
      "title" : "Role Configuration",
      "propertyOrder" : 6,
      "properties" : {
        "sun-idrepo-ldapv3-config-filterroles-search-attribute" : {
          "title" : "LDAP Filter Roles Search Attribute",
          "description" : "",
          "propertyOrder" : 4300,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-nsrole" : {
          "title" : "Attribute Name for Filtered Role Membership",
          "description" : "",
          "propertyOrder" : 4700,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-role-objectclass" : {
          "title" : "LDAP Roles Object Class",
          "description" : "",
          "propertyOrder" : 4100,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-nsroledn" : {
```

```
          "title" : "Attribute Name of Role Membership.",
          "description" : "",
          "propertyOrder" : 4800,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-filterrole-objectclass" : {
          "title" : "LDAP Filter Roles Object Class",
          "description" : "",
          "propertyOrder" : 4500,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-roles-search-filter" : {
          "title" : "LDAP Roles Search Filter",
          "description" : "",
          "propertyOrder" : 4000,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-filterroles-search-filter" : {
          "title" : "LDAP Filter Roles Search Filter",
          "description" : "",
          "propertyOrder" : 4400,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-filterrole-attributes" : {
          "title" : "LDAP Filter Roles Attributes",
          "description" : "",
          "propertyOrder" : 4600,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-roles-search-attribute" : {
          "title" : "LDAP Roles Search Attribute",
          "description" : "",
          "propertyOrder" : 3900,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-nsrolefilter" : {
          "title" : "Attribute Name of Filtered Role Filter",
          "description" : "",
          "propertyOrder" : 4900,
          "required" : false,
          "type" : "string",
```

```
        "exampleValue" : ""
      },
      "sun-idrepo-ldapv3-config-role-attributes" : {
        "title" : "LDAP Roles Attributes",
        "description" : "",
        "propertyOrder" : 4200,
        "required" : false,
        "items" : {
          "type" : "string"
        },
        "type" : "array",
        "exampleValue" : ""
      }
    }
  },
  "pluginconfig" : {
    "type" : "object",
    "title" : "Plug-in Configuration",
    "propertyOrder" : 2,
    "properties" : {
      "sunIdRepoSupportedOperations" : {
        "title" : "LDAPv3 Plug-in Supported Types and Operations",
        "description" : "",
        "propertyOrder" : 1900,
        "required" : false,
        "items" : {
          "type" : "string"
        },
        "type" : "array",
        "exampleValue" : ""
      },
      "sunIdRepoClass" : {
        "title" : "LDAPv3 Repository Plug-in Class Name",
        "description" : "",
        "propertyOrder" : 1700,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
      },
      "sunIdRepoAttributeMapping" : {
        "title" : "Attribute Name Mapping",
        "description" : "",
        "propertyOrder" : 1800,
        "required" : false,
        "items" : {
          "type" : "string"
        },
        "type" : "array",
        "exampleValue" : ""
      }
    }
  },
  "ldapsettings" : {
    "type" : "object",
    "title" : "Server Settings",
    "propertyOrder" : 0,
    "properties" : {
      "sun-idrepo-ldapv3-config-connection-mode" : {
        "title" : "LDAP Connection Mode",
```

```
          "description" : "Defines which protocol/operation is used to establish the connection to
the LDAP Directory Server.<br><br>If 'LDAP' is selected, the connection <b>won't be secured</b> and
passwords are transferred in <b>cleartext</b> over the network.<br/> If 'LDAPS' is selected, the
connection is secured via SSL or TLS. <br/> If 'StartTLS' is selected, the connection is secured by
using StartTLS extended operation.",
          "propertyOrder" : 1000,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "openam-idrepo-ldapv3-affinity-enabled" : {
          "title" : "Affinity Enabled",
          "description" : "Enables affinity based request load balancing when accessing the user store
servers (based on DN). It is imperative that the connection string setting is set to the same value
for all OpenAM servers in the deployment when this feature is enabled.",
          "propertyOrder" : 6200,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-connection_pool_min_size" : {
          "title" : "LDAP Connection Pool Minimum Size",
          "description" : "",
          "propertyOrder" : 1100,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-organization_name" : {
          "title" : "LDAP Organization DN",
          "description" : "",
          "propertyOrder" : 900,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-authid" : {
          "title" : "LDAP Bind DN",
          "description" : "A user or admin with sufficient access rights to perform the supported
operations.",
          "propertyOrder" : 700,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-time-limit" : {
          "title" : "Search Timeout",
          "description" : "In seconds.",
          "propertyOrder" : 1600,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-authpw" : {
          "title" : "LDAP Bind Password",
          "description" : "",
          "propertyOrder" : 800,
          "required" : false,
          "type" : "string",
```

```
          "format" : "password",
          "exampleValue" : ""
        },
        "openam-idrepo-ldapv3-behera-support-enabled" : {
          "title" : "Behera Support Enabled",
          "description" : "When enabled, Behera draft control will be used in the outgoing requests
for operations that may modify password value. This will allow OpenAM to display password policy
related error messages when password policies are not met.",
          "propertyOrder" : 6100,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "openam-idrepo-ldapv3-heartbeat-interval" : {
          "title" : "LDAP Connection Heartbeat Interval",
          "description" : "Specifies how often should OpenAM send a heartbeat request to the
directory.<br><br>This setting controls how often OpenAM <b>should</b> send a heartbeat search
request to the configured directory. If a connection becomes unresponsive (e.g. due to a network
error) then it may take up to the interval period before the problem is detected. Use along with the
Heartbeat Time Unit parameter to define the exact interval. Zero or negative value will result in
disabling heartbeat requests.",
          "propertyOrder" : 1300,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "openam-idrepo-ldapv3-heartbeat-timeunit" : {
          "title" : "LDAP Connection Heartbeat Time Unit",
          "description" : "Defines the time unit corresponding to the Heartbeat Interval
setting.<br><br>This setting controls how often OpenAM <b>should</b> send a heartbeat search request
to the configured directory. If a connection becomes unresponsive (e.g. due to a network error) then
it may take up to the interval period before the problem is detected. Use along with the Heartbeat
Interval parameter to define the exact interval.",
          "propertyOrder" : 1400,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-search-scope" : {
          "title" : "LDAPv3 Plug-in Search Scope",
          "description" : "",
          "propertyOrder" : 2000,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-max-result" : {
          "title" : "Maximum Results Returned from Search",
          "description" : "",
          "propertyOrder" : 1500,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-ldap-server" : {
          "title" : "LDAP Server",
          "description" : "Format: LDAP server host name:port | server_ID | site_ID",
          "propertyOrder" : 600,
          "required" : true,
```

```
          "items" : {
            "type" : "string"
          },
          "minItems" : 1,
          "type" : "array",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-connection_pool_max_size" : {
          "title" : "LDAP Connection Pool Maximum Size",
          "description" : "",
          "propertyOrder" : 1200,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        }
      }
    },
    "groupconfig" : {
      "type" : "object",
      "title" : "Group Configuration",
      "propertyOrder" : 5,
      "properties" : {
        "sun-idrepo-ldapv3-config-group-attributes" : {
          "title" : "LDAP Groups Attributes",
          "description" : "",
          "propertyOrder" : 3400,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-groups-search-attribute" : {
          "title" : "LDAP Groups Search Attribute",
          "description" : "",
          "propertyOrder" : 2900,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-memberurl" : {
          "title" : "Attribute Name of Group Member URL",
          "description" : "",
          "propertyOrder" : 3700,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-uniquemember" : {
          "title" : "Attribute Name of Unique Member",
          "description" : "",
          "propertyOrder" : 3600,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-group-objectclass" : {
          "title" : "LDAP Groups Object Class",
```

```
          "description" : "",
          "propertyOrder" : 3300,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-group-container-name" : {
          "title" : "LDAP Groups Container Naming Attribute",
          "description" : "",
          "propertyOrder" : 3100,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-group-container-value" : {
          "title" : "LDAP Groups Container Value",
          "description" : "",
          "propertyOrder" : 3200,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-groups-search-filter" : {
          "title" : "LDAP Groups Search Filter",
          "description" : "",
          "propertyOrder" : 3000,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-memberof" : {
          "title" : "Attribute Name for Group Membership",
          "description" : "",
          "propertyOrder" : 3500,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "userconfig" : {
      "type" : "object",
      "title" : "User Configuration",
      "propertyOrder" : 3,
      "properties" : {
        "sun-idrepo-ldapv3-config-users-search-attribute" : {
          "title" : "LDAP Users  Search Attribute",
          "description" : "",
          "propertyOrder" : 2100,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-people-container-name" : {
          "title" : "LDAP People Container Naming Attribute",
          "description" : "",
```

```
          "propertyOrder" : 5000,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-isactive" : {
          "title" : "Attribute Name of User Status",
          "description" : "",
          "propertyOrder" : 2600,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-user-attributes" : {
          "title" : "LDAP User Attributes",
          "description" : "",
          "propertyOrder" : 2400,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-users-search-filter" : {
          "title" : "LDAP Users  Search Filter",
          "description" : "",
          "propertyOrder" : 2200,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-createuser-attr-mapping" : {
          "title" : "Create User Attribute Mapping",
          "description" : "Format: attribute name or TargetAttributeName=SourceAttributeName",
          "propertyOrder" : 2500,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-people-container-value" : {
          "title" : "LDAP People Container Value",
          "description" : "",
          "propertyOrder" : 5100,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-auth-kba-index-attr" : {
          "title" : "Knowledge Based Authentication Active Index",
          "description" : "",
          "propertyOrder" : 5400,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
```

```
        "sun-idrepo-ldapv3-config-user-objectclass" : {
          "title" : "LDAP User Object Class",
          "description" : "",
          "propertyOrder" : 2300,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-auth-kba-attr" : {
          "title" : "Knowledge Based Authentication Attribute Name",
          "description" : "",
          "propertyOrder" : 5300,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-inactive" : {
          "title" : "User Status Inactive Value",
          "description" : "",
          "propertyOrder" : 2800,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-auth-kba-attempts-attr" : {
          "title" : "Knowledge Based Authentication Attempts Attribute Name",
          "description" : "",
          "propertyOrder" : 5410,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-active" : {
          "title" : "User Status Active Value",
          "description" : "",
          "propertyOrder" : 2700,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "persistentsearch" : {
      "type" : "object",
      "title" : "Persistent Search Controls",
      "propertyOrder" : 7,
      "properties" : {
        "sun-idrepo-ldapv3-config-psearchbase" : {
          "title" : "Persistent Search Base DN",
          "description" : "",
          "propertyOrder" : 5500,
          "required" : false,
          "type" : "string",
```

```
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-psearch-filter" : {
          "title" : "Persistent Search Filter",
          "description" : "",
          "propertyOrder" : 5600,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-psearch-scope" : {
          "title" : "Persistent Search Scope",
          "description" : "",
          "propertyOrder" : 5700,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "cachecontrol" : {
      "type" : "object",
      "title" : "Cache Control",
      "propertyOrder" : 9,
      "properties" : {
        "sun-idrepo-ldapv3-dncache-size" : {
          "title" : "DN Cache Size",
          "description" : "In DN items, only used when DN Cache is enabled.",
          "propertyOrder" : 6000,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-dncache-enabled" : {
          "title" : "DN Cache",
          "description" : "Used to enable/disable the DN Cache within the OpenAM repository
implementation.<br><br>The DN Cache is used to cache DN lookups which tend to happen in bursts during
authentication. The DN Cache can become out of date when a user is moved or renamed in the underlying
LDAP store and this is not reflected in a persistent search result. Enable when the underlying LDAP
store supports persistent search and move/rename (mod_dn) results are available.",
          "propertyOrder" : 5900,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        }
      }
    },
    "errorhandling" : {
      "type" : "object",
      "title" : "Error Handling Configuration",
      "propertyOrder" : 8,
      "properties" : {
        "com.iplanet.am.ldap.connection.delay.between.retries" : {
          "title" : "The Delay Time Between Retries",
          "description" : "In milliseconds.",
          "propertyOrder" : 5800,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
```

```
        }
      }
    },
    "authentication" : {
      "type" : "object",
      "title" : "Authentication Configuration",
      "propertyOrder" : 4,
      "properties" : {
        "sun-idrepo-ldapv3-config-auth-naming-attr" : {
          "title" : "Authentication Naming Attribute",
          "description" : "",
          "propertyOrder" : 5200,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    }
  }
}
```

delete

Usage:

```
am> delete SunDSWithOpenAMSchema --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action SunDSWithOpenAMSchema --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action SunDSWithOpenAMSchema --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action SunDSWithOpenAMSchema --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query SunDSWithOpenAMSchema --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read SunDSWithOpenAMSchema --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update SunDSWithOpenAMSchema --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "roleconfig" : {
      "type" : "object",
      "title" : "Role Configuration",
      "propertyOrder" : 6,
```

```
      "properties" : {
        "sun-idrepo-ldapv3-config-filterroles-search-attribute" : {
          "title" : "LDAP Filter Roles Search Attribute",
          "description" : "",
          "propertyOrder" : 4300,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-nsrole" : {
          "title" : "Attribute Name for Filtered Role Membership",
          "description" : "",
          "propertyOrder" : 4700,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-role-objectclass" : {
          "title" : "LDAP Roles Object Class",
          "description" : "",
          "propertyOrder" : 4100,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-nsroledn" : {
          "title" : "Attribute Name of Role Membership.",
          "description" : "",
          "propertyOrder" : 4800,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-filterrole-objectclass" : {
          "title" : "LDAP Filter Roles Object Class",
          "description" : "",
          "propertyOrder" : 4500,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-roles-search-filter" : {
          "title" : "LDAP Roles Search Filter",
          "description" : "",
          "propertyOrder" : 4000,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-filterroles-search-filter" : {
          "title" : "LDAP Filter Roles Search Filter",
          "description" : "",
          "propertyOrder" : 4400,
```

```
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-filterrole-attributes" : {
          "title" : "LDAP Filter Roles Attributes",
          "description" : "",
          "propertyOrder" : 4600,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-roles-search-attribute" : {
          "title" : "LDAP Roles Search Attribute",
          "description" : "",
          "propertyOrder" : 3900,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-nsrolefilter" : {
          "title" : "Attribute Name of Filtered Role Filter",
          "description" : "",
          "propertyOrder" : 4900,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-role-attributes" : {
          "title" : "LDAP Roles Attributes",
          "description" : "",
          "propertyOrder" : 4200,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        }
      }
    },
    "pluginconfig" : {
      "type" : "object",
      "title" : "Plug-in Configuration",
      "propertyOrder" : 2,
      "properties" : {
        "sunIdRepoSupportedOperations" : {
          "title" : "LDAPv3 Plug-in Supported Types and Operations",
          "description" : "",
          "propertyOrder" : 1900,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
```

```
        },
        "sunIdRepoClass" : {
          "title" : "LDAPv3 Repository Plug-in Class Name",
          "description" : "",
          "propertyOrder" : 1700,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "sunIdRepoAttributeMapping" : {
          "title" : "Attribute Name Mapping",
          "description" : "",
          "propertyOrder" : 1800,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        }
      }
    },
    "ldapsettings" : {
      "type" : "object",
      "title" : "Server Settings",
      "propertyOrder" : 0,
      "properties" : {
        "sun-idrepo-ldapv3-config-connection-mode" : {
          "title" : "LDAP Connection Mode",
          "description" : "Defines which protocol/operation is used to establish the connection to
the LDAP Directory Server.<br><br>If 'LDAP' is selected, the connection <b>won't be secured</b> and
passwords are transferred in <b>cleartext</b> over the network.<br/> If 'LDAPS' is selected, the
connection is secured via SSL or TLS. <br/> If 'StartTLS' is selected, the connection is secured by
using StartTLS extended operation.",
          "propertyOrder" : 1000,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "openam-idrepo-ldapv3-affinity-enabled" : {
          "title" : "Affinity Enabled",
          "description" : "Enables affinity based request load balancing when accessing the user store
servers (based on DN). It is imperative that the connection string setting is set to the same value
for all OpenAM servers in the deployment when this feature is enabled.",
          "propertyOrder" : 6200,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-connection_pool_min_size" : {
          "title" : "LDAP Connection Pool Minimum Size",
          "description" : "",
          "propertyOrder" : 1100,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-organization_name" : {
          "title" : "LDAP Organization DN",
```

```
          "description" : "",
          "propertyOrder" : 900,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-authid" : {
          "title" : "LDAP Bind DN",
          "description" : "A user or admin with sufficient access rights to perform the supported
operations.",
          "propertyOrder" : 700,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-time-limit" : {
          "title" : "Search Timeout",
          "description" : "In seconds.",
          "propertyOrder" : 1600,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-authpw" : {
          "title" : "LDAP Bind Password",
          "description" : "",
          "propertyOrder" : 800,
          "required" : false,
          "type" : "string",
          "format" : "password",
          "exampleValue" : ""
        },
        "openam-idrepo-ldapv3-behera-support-enabled" : {
          "title" : "Behera Support Enabled",
          "description" : "When enabled, Behera draft control will be used in the outgoing requests
for operations that may modify password value. This will allow OpenAM to display password policy
related error messages when password policies are not met.",
          "propertyOrder" : 6100,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "openam-idrepo-ldapv3-heartbeat-interval" : {
          "title" : "LDAP Connection Heartbeat Interval",
          "description" : "Specifies how often should OpenAM send a heartbeat request to the
directory.<br><br>This setting controls how often OpenAM <b>should</b> send a heartbeat search
request to the configured directory. If a connection becomes unresponsive (e.g. due to a network
error) then it may take up to the interval period before the problem is detected. Use along with the
Heartbeat Time Unit parameter to define the exact interval. Zero or negative value will result in
disabling heartbeat requests.",
          "propertyOrder" : 1300,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "openam-idrepo-ldapv3-heartbeat-timeunit" : {
          "title" : "LDAP Connection Heartbeat Time Unit",
          "description" : "Defines the time unit corresponding to the Heartbeat Interval
setting.<br><br>This setting controls how often OpenAM <b>should</b> send a heartbeat search request
```

```
to the configured directory. If a connection becomes unresponsive (e.g. due to a network error) then
it may take up to the interval period before the problem is detected. Use along with the Heartbeat
Interval parameter to define the exact interval.",
          "propertyOrder" : 1400,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-search-scope" : {
          "title" : "LDAPv3 Plug-in Search Scope",
          "description" : "",
          "propertyOrder" : 2000,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-max-result" : {
          "title" : "Maximum Results Returned from Search",
          "description" : "",
          "propertyOrder" : 1500,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-ldap-server" : {
          "title" : "LDAP Server",
          "description" : "Format: LDAP server host name:port | server_ID | site_ID",
          "propertyOrder" : 600,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "minItems" : 1,
          "type" : "array",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-connection_pool_max_size" : {
          "title" : "LDAP Connection Pool Maximum Size",
          "description" : "",
          "propertyOrder" : 1200,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        }
      }
    },
    "groupconfig" : {
      "type" : "object",
      "title" : "Group Configuration",
      "propertyOrder" : 5,
      "properties" : {
        "sun-idrepo-ldapv3-config-group-attributes" : {
          "title" : "LDAP Groups Attributes",
          "description" : "",
          "propertyOrder" : 3400,
          "required" : false,
          "items" : {
            "type" : "string"
          },
```

```
          "type" : "array",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-groups-search-attribute" : {
          "title" : "LDAP Groups Search Attribute",
          "description" : "",
          "propertyOrder" : 2900,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-memberurl" : {
          "title" : "Attribute Name of Group Member URL",
          "description" : "",
          "propertyOrder" : 3700,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-uniquemember" : {
          "title" : "Attribute Name of Unique Member",
          "description" : "",
          "propertyOrder" : 3600,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-group-objectclass" : {
          "title" : "LDAP Groups Object Class",
          "description" : "",
          "propertyOrder" : 3300,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-group-container-name" : {
          "title" : "LDAP Groups Container Naming Attribute",
          "description" : "",
          "propertyOrder" : 3100,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-group-container-value" : {
          "title" : "LDAP Groups Container Value",
          "description" : "",
          "propertyOrder" : 3200,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-groups-search-filter" : {
          "title" : "LDAP Groups Search Filter",
          "description" : "",
          "propertyOrder" : 3000,
          "required" : false,
```

```
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-memberof" : {
          "title" : "Attribute Name for Group Membership",
          "description" : "",
          "propertyOrder" : 3500,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "userconfig" : {
      "type" : "object",
      "title" : "User Configuration",
      "propertyOrder" : 3,
      "properties" : {
        "sun-idrepo-ldapv3-config-users-search-attribute" : {
          "title" : "LDAP Users  Search Attribute",
          "description" : "",
          "propertyOrder" : 2100,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-people-container-name" : {
          "title" : "LDAP People Container Naming Attribute",
          "description" : "",
          "propertyOrder" : 5000,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-isactive" : {
          "title" : "Attribute Name of User Status",
          "description" : "",
          "propertyOrder" : 2600,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-user-attributes" : {
          "title" : "LDAP User Attributes",
          "description" : "",
          "propertyOrder" : 2400,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-users-search-filter" : {
          "title" : "LDAP Users  Search Filter",
          "description" : "",
          "propertyOrder" : 2200,
          "required" : false,
          "type" : "string",
```

```
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-createuser-attr-mapping" : {
          "title" : "Create User Attribute Mapping",
          "description" : "Format: attribute name or TargetAttributeName=SourceAttributeName",
          "propertyOrder" : 2500,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-people-container-value" : {
          "title" : "LDAP People Container Value",
          "description" : "",
          "propertyOrder" : 5100,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-auth-kba-index-attr" : {
          "title" : "Knowledge Based Authentication Active Index",
          "description" : "",
          "propertyOrder" : 5400,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-user-objectclass" : {
          "title" : "LDAP User Object Class",
          "description" : "",
          "propertyOrder" : 2300,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-auth-kba-attr" : {
          "title" : "Knowledge Based Authentication Attribute Name",
          "description" : "",
          "propertyOrder" : 5300,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-inactive" : {
          "title" : "User Status Inactive Value",
          "description" : "",
          "propertyOrder" : 2800,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
```

```
        "sun-idrepo-ldapv3-config-auth-kba-attempts-attr" : {
          "title" : "Knowledge Based Authentication Attempts Attribute Name",
          "description" : "",
          "propertyOrder" : 5410,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-active" : {
          "title" : "User Status Active Value",
          "description" : "",
          "propertyOrder" : 2700,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "persistentsearch" : {
      "type" : "object",
      "title" : "Persistent Search Controls",
      "propertyOrder" : 7,
      "properties" : {
        "sun-idrepo-ldapv3-config-psearchbase" : {
          "title" : "Persistent Search Base DN",
          "description" : "",
          "propertyOrder" : 5500,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-psearch-filter" : {
          "title" : "Persistent Search Filter",
          "description" : "",
          "propertyOrder" : 5600,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-psearch-scope" : {
          "title" : "Persistent Search Scope",
          "description" : "",
          "propertyOrder" : 5700,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "cachecontrol" : {
      "type" : "object",
      "title" : "Cache Control",
      "propertyOrder" : 9,
      "properties" : {
        "sun-idrepo-ldapv3-dncache-size" : {
          "title" : "DN Cache Size",
          "description" : "In DN items, only used when DN Cache is enabled.",
          "propertyOrder" : 6000,
          "required" : false,
```

```
          "type" : "integer",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-dncache-enabled" : {
          "title" : "DN Cache",
          "description" : "Used to enable/disable the DN Cache within the OpenAM repository
 implementation.<br><br>The DN Cache is used to cache DN lookups which tend to happen in bursts during
 authentication. The DN Cache can become out of date when a user is moved or renamed in the underlying
 LDAP store and this is not reflected in a persistent search result. Enable when the underlying LDAP
 store supports persistent search and move/rename (mod_dn) results are available.",
          "propertyOrder" : 5900,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        }
      }
    },
    "errorhandling" : {
      "type" : "object",
      "title" : "Error Handling Configuration",
      "propertyOrder" : 8,
      "properties" : {
        "com.iplanet.am.ldap.connection.delay.between.retries" : {
          "title" : "The Delay Time Between Retries",
          "description" : "In milliseconds.",
          "propertyOrder" : 5800,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        }
      }
    },
    "authentication" : {
      "type" : "object",
      "title" : "Authentication Configuration",
      "propertyOrder" : 4,
      "properties" : {
        "sun-idrepo-ldapv3-config-auth-naming-attr" : {
          "title" : "Authentication Naming Attribute",
          "description" : "",
          "propertyOrder" : 5200,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    }
  }
}
```

SupportedIds

Global Operations

Resource path: `/global-config/services/id-repositories/SupportedIdentities`

Resource version: `1.0`

create

Usage:

```
am> create SupportedIds --global --id id --body body
```

Parameters:

`--id`

The unique identifier for the resource.

`--body`

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object"
}
```

delete

Usage:

```
am> delete SupportedIds --global --id id
```

Parameters:

`--id`

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action SupportedIds --global --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action SupportedIds --global --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action SupportedIds --global --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query SupportedIds --global --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read SupportedIds --global --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update SupportedIds --global --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object"
}
```

Syslog

Realm Operations

Resource path: `/realm-config/services/audit/Syslog`

Resource version: `1.0`

create

Usage:

```
am> create Syslog --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "sysLogConfig" : {
      "type" : "object",
      "title" : "Syslog Configuration",
      "propertyOrder" : 2,
      "properties" : {
        "port" : {
          "title" : "Server port",
          "description" : "Port number of receiving syslog server.",
          "propertyOrder" : 2500,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "host" : {
          "title" : "Server hostname",
          "description" : "Host name or IP address of receiving syslog server.",
          "propertyOrder" : 2400,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
```

```
        },
        "facility" : {
          "title" : "Facility",
          "description" : "Syslog facility value to apply to all events.",
          "propertyOrder" : 2800,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "transportProtocol" : {
          "title" : "Transport Protocol",
          "description" : "",
          "propertyOrder" : 2600,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "connectTimeout" : {
          "title" : "Connection timeout",
          "description" : "Timeout for connecting to syslog server, in seconds.",
          "propertyOrder" : 2700,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "commonHandler" : {
      "type" : "object",
      "title" : "General Handler Configuration",
      "propertyOrder" : 0,
      "properties" : {
        "enabled" : {
          "title" : "Enabled",
          "description" : "Enables or disables an audit event handler.",
          "propertyOrder" : 2200,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "topics" : {
          "title" : "Topics",
          "description" : "List of topics handled by an audit event handler.",
          "propertyOrder" : 2300,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        }
      }
    },
    "sysLogBuffering" : {
      "type" : "object",
      "title" : "Buffering",
      "propertyOrder" : 3,
      "properties" : {
        "bufferingMaxSize" : {
```

```
          "title" : "Buffer Size",
          "description" : "Maximum number of events that can be buffered (default/minimum: 5000)",
          "propertyOrder" : 2950,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "bufferingEnabled" : {
          "title" : "Buffering Enabled",
          "description" : "Enables or disables audit event buffering.",
          "propertyOrder" : 2900,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        }
      }
    },
    "commonHandlerPlugin" : {
      "type" : "object",
      "title" : "Audit Event Handler Factory",
      "propertyOrder" : 1,
      "properties" : {
        "handlerFactory" : {
          "title" : "Factory Class Name",
          "description" : "The fully qualified class name of the factory
 responsible for creating the Audit Event Handler. The class must implement
 <code>org.forgerock.openam.audit.AuditEventHandlerFactory</code>.",
          "propertyOrder" : 3000,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    }
  }
}
```

delete

Usage:

```
am> delete Syslog --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action Syslog --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action Syslog --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action Syslog --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query Syslog --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read Syslog --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update Syslog --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "sysLogConfig" : {
      "type" : "object",
      "title" : "Syslog Configuration",
      "propertyOrder" : 2,
      "properties" : {
        "port" : {
          "title" : "Server port",
          "description" : "Port number of receiving syslog server.",
          "propertyOrder" : 2500,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "host" : {
          "title" : "Server hostname",
          "description" : "Host name or IP address of receiving syslog server.",
          "propertyOrder" : 2400,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "facility" : {
          "title" : "Facility",
          "description" : "Syslog facility value to apply to all events.",
          "propertyOrder" : 2800,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "transportProtocol" : {
          "title" : "Transport Protocol",
          "description" : "",
          "propertyOrder" : 2600,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "connectTimeout" : {
          "title" : "Connection timeout",
          "description" : "Timeout for connecting to syslog server, in seconds.",
          "propertyOrder" : 2700,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      }
```

```
    },
    "commonHandler" : {
      "type" : "object",
      "title" : "General Handler Configuration",
      "propertyOrder" : 0,
      "properties" : {
        "enabled" : {
          "title" : "Enabled",
          "description" : "Enables or disables an audit event handler.",
          "propertyOrder" : 2200,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "topics" : {
          "title" : "Topics",
          "description" : "List of topics handled by an audit event handler.",
          "propertyOrder" : 2300,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        }
      }
    },
    "sysLogBuffering" : {
      "type" : "object",
      "title" : "Buffering",
      "propertyOrder" : 3,
      "properties" : {
        "bufferingMaxSize" : {
          "title" : "Buffer Size",
          "description" : "Maximum number of events that can be buffered (default/minimum: 5000)",
          "propertyOrder" : 2950,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "bufferingEnabled" : {
          "title" : "Buffering Enabled",
          "description" : "Enables or disables audit event buffering.",
          "propertyOrder" : 2900,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        }
      }
    },
    "commonHandlerPlugin" : {
      "type" : "object",
      "title" : "Audit Event Handler Factory",
      "propertyOrder" : 1,
      "properties" : {
        "handlerFactory" : {
          "title" : "Factory Class Name",
```

```
          "description" : "The fully qualified class name of the factory
 responsible for creating the Audit Event Handler. The class must implement
 <code>org.forgerock.openam.audit.AuditEventHandlerFactory</code>.",
          "propertyOrder" : 3000,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    }
  }
}
```

Global Operations

Resource path: `/global-config/services/audit/Syslog`

Resource version: `1.0`

create

Usage:

```
am> create Syslog --global --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "sysLogBuffering" : {
      "type" : "object",
      "title" : "Buffering",
      "propertyOrder" : 3,
      "properties" : {
        "bufferingMaxSize" : {
          "title" : "Buffer Size",
          "description" : "Maximum number of events that can be buffered (default/minimum: 5000)",
          "propertyOrder" : 2950,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "bufferingEnabled" : {
          "title" : "Buffering Enabled",
          "description" : "Enables or disables audit event buffering.",
```

```
        "propertyOrder" : 2900,
        "required" : true,
        "type" : "boolean",
        "exampleValue" : ""
      }
    }
  },
  "sysLogConfig" : {
    "type" : "object",
    "title" : "Syslog Configuration",
    "propertyOrder" : 2,
    "properties" : {
      "host" : {
        "title" : "Server hostname",
        "description" : "Host name or IP address of receiving syslog server.",
        "propertyOrder" : 2400,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
      },
      "facility" : {
        "title" : "Facility",
        "description" : "Syslog facility value to apply to all events.",
        "propertyOrder" : 2800,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
      },
      "transportProtocol" : {
        "title" : "Transport Protocol",
        "description" : "",
        "propertyOrder" : 2600,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
      },
      "connectTimeout" : {
        "title" : "Connection timeout",
        "description" : "Timeout for connecting to syslog server, in seconds.",
        "propertyOrder" : 2700,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
      },
      "port" : {
        "title" : "Server port",
        "description" : "Port number of receiving syslog server.",
        "propertyOrder" : 2500,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
      }
    }
  },
  "commonHandler" : {
    "type" : "object",
    "title" : "General Handler Configuration",
    "propertyOrder" : 0,
    "properties" : {
```

```
        "topics" : {
          "title" : "Topics",
          "description" : "List of topics handled by an audit event handler.",
          "propertyOrder" : 2300,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "enabled" : {
          "title" : "Enabled",
          "description" : "Enables or disables an audit event handler.",
          "propertyOrder" : 2200,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        }
      }
    },
    "commonHandlerPlugin" : {
      "type" : "object",
      "title" : "Audit Event Handler Factory",
      "propertyOrder" : 1,
      "properties" : {
        "handlerFactory" : {
          "title" : "Factory Class Name",
          "description" : "The fully qualified class name of the factory
 responsible for creating the Audit Event Handler. The class must implement
 <code>org.forgerock.openam.audit.AuditEventHandlerFactory</code>.",
          "propertyOrder" : 3000,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    }
  }
}
```

delete

Usage:

```
am> delete Syslog --global --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action Syslog --global --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action Syslog --global --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action Syslog --global --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query Syslog --global --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read Syslog --global --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update Syslog --global --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "sysLogBuffering" : {
      "type" : "object",
      "title" : "Buffering",
      "propertyOrder" : 3,
      "properties" : {
        "bufferingMaxSize" : {
          "title" : "Buffer Size",
          "description" : "Maximum number of events that can be buffered (default/minimum: 5000)",
          "propertyOrder" : 2950,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "bufferingEnabled" : {
          "title" : "Buffering Enabled",
          "description" : "Enables or disables audit event buffering.",
          "propertyOrder" : 2900,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        }
      }
    },
    "sysLogConfig" : {
      "type" : "object",
      "title" : "Syslog Configuration",
      "propertyOrder" : 2,
      "properties" : {
        "host" : {
          "title" : "Server hostname",
          "description" : "Host name or IP address of receiving syslog server.",
          "propertyOrder" : 2400,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "facility" : {
          "title" : "Facility",
          "description" : "Syslog facility value to apply to all events.",
```

```
          "propertyOrder" : 2800,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "transportProtocol" : {
          "title" : "Transport Protocol",
          "description" : "",
          "propertyOrder" : 2600,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "connectTimeout" : {
          "title" : "Connection timeout",
          "description" : "Timeout for connecting to syslog server, in seconds.",
          "propertyOrder" : 2700,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "port" : {
          "title" : "Server port",
          "description" : "Port number of receiving syslog server.",
          "propertyOrder" : 2500,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "commonHandler" : {
      "type" : "object",
      "title" : "General Handler Configuration",
      "propertyOrder" : 0,
      "properties" : {
        "topics" : {
          "title" : "Topics",
          "description" : "List of topics handled by an audit event handler.",
          "propertyOrder" : 2300,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "enabled" : {
          "title" : "Enabled",
          "description" : "Enables or disables an audit event handler.",
          "propertyOrder" : 2200,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        }
      }
    },
    "commonHandlerPlugin" : {
      "type" : "object",
```

```
      "title" : "Audit Event Handler Factory",
      "propertyOrder" : 1,
      "properties" : {
        "handlerFactory" : {
          "title" : "Factory Class Name",
          "description" : "The fully qualified class name of the factory
 responsible for creating the Audit Event Handler. The class must implement
 <code>org.forgerock.openam.audit.AuditEventHandlerFactory</code>.",
          "propertyOrder" : 3000,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    }
  }
}
```

TermsAndConditionsDecision

Realm Operations

Resource path: `/realm-config/authentication/authenticationtrees/nodes/TermsAndConditionsDecisionNode`

Resource version: `1.0`

create

Usage:

```
am> create TermsAndConditionsDecision --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "identityAttribute" : {
      "title" : "Identity Attribute",
      "description" : "The attribute to query for the IDM object.",
      "propertyOrder" : 100,
      "type" : "string",
      "exampleValue" : ""
    }
  },
  "required" : [ "identityAttribute" ]
}
```

delete

Usage:

```
am> delete TermsAndConditionsDecision --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action TermsAndConditionsDecision --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action TermsAndConditionsDecision --realm Realm --actionName getCreatableTypes
```

listOutcomes

List the available outcomes for the node type.

Usage:

```
am> action TermsAndConditionsDecision --realm Realm --body body --actionName listOutcomes
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "title" : "Some configuration of the node. This does not need to be complete against the
 configuration schema."
}
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action TermsAndConditionsDecision --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query TermsAndConditionsDecision --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read TermsAndConditionsDecision --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update TermsAndConditionsDecision --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "identityAttribute" : {
      "title" : "Identity Attribute",
      "description" : "The attribute to query for the IDM object.",
      "propertyOrder" : 100,
      "type" : "string",
      "exampleValue" : ""
    }
  },
  "required" : [ "identityAttribute" ]
}
```

TimeSinceDecision

Realm Operations

Resource path: `/realm-config/authentication/authenticationtrees/nodes/TimeSinceDecisionNode`

Resource version: `1.0`

create

Usage:

```
am> create TimeSinceDecision --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "elapsedTime" : {
      "title" : "Elapsed Time",
      "description" : "The amount of elapsed time, in minutes, to compare.",
      "propertyOrder" : 100,
      "type" : "string",
      "exampleValue" : ""
    },
    "identityAttribute" : {
      "title" : "Identity Attribute",
      "description" : "The attribute to query in the IDM object.",
      "propertyOrder" : 300,
      "type" : "string",
      "exampleValue" : ""
    }
  },
  "required" : [ "elapsedTime", "identityAttribute" ]
}
```

delete

Usage:

```
am> delete TimeSinceDecision --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action TimeSinceDecision --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action TimeSinceDecision --realm Realm --actionName getCreatableTypes
```

listOutcomes

List the available outcomes for the node type.

Usage:

```
am> action TimeSinceDecision --realm Realm --body body --actionName listOutcomes
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "title" : "Some configuration of the node. This does not need to be complete against the
 configuration schema."
}
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action TimeSinceDecision --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query TimeSinceDecision --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read TimeSinceDecision --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update TimeSinceDecision --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "elapsedTime" : {
      "title" : "Elapsed Time",
      "description" : "The amount of elapsed time, in minutes, to compare.",
      "propertyOrder" : 100,
      "type" : "string",
      "exampleValue" : ""
    },
    "identityAttribute" : {
      "title" : "Identity Attribute",
      "description" : "The attribute to query in the IDM object.",
      "propertyOrder" : 300,
      "type" : "string",
      "exampleValue" : ""
    }
  },
  "required" : [ "elapsedTime", "identityAttribute" ]
}
```

TimerStart

Realm Operations

Resource path: `/realm-config/authentication/authenticationtrees/nodes/TimerStartNode`

Resource version: `1.0`

create

Usage:

```
am> create TimerStart --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "startTimeProperty" : {
      "title" : "Start Time Property",
      "description" : "Identifier of property into which start time should be stored by this node.",
      "propertyOrder" : 100,
      "type" : "string",
      "exampleValue" : ""
    }
  },
  "required" : [ "startTimeProperty" ]
}
```

delete

Usage:

```
am> delete TimerStart --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action TimerStart --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action TimerStart --realm Realm --actionName getCreatableTypes
```

listOutcomes

List the available outcomes for the node type.

Usage:

```
am> action TimerStart --realm Realm --body body --actionName listOutcomes
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "title" : "Some configuration of the node. This does not need to be complete against the
 configuration schema."
}
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action TimerStart --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query TimerStart --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read TimerStart --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update TimerStart --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "startTimeProperty" : {
      "title" : "Start Time Property",
      "description" : "Identifier of property into which start time should be stored by this node.",
      "propertyOrder" : 100,
      "type" : "string",
      "exampleValue" : ""
    }
  },
  "required" : [ "startTimeProperty" ]
}
```

TimerStop

Realm Operations

Resource path: `/realm-config/authentication/authenticationtrees/nodes/TimerStopNode`

Resource version: `1.0`

create

Usage:

```
am> create TimerStop --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "startTimeProperty" : {
      "title" : "Start Time Property",
      "description" : "Identifier of property in which start time should have been stored by a \"Timer
 Start\" node.",
      "propertyOrder" : 100,
      "type" : "string",
      "exampleValue" : ""
    },
    "metricKey" : {
      "title" : "Metric Key",
      "description" : "Identifier of metric to update when this node is processed.",
      "propertyOrder" : 200,
      "type" : "string",
      "exampleValue" : ""
    }
  },
  "required" : [ "metricKey", "startTimeProperty" ]
}
```

delete

Usage:

```
am> delete TimerStop --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action TimerStop --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action TimerStop --realm Realm --actionName getCreatableTypes
```

listOutcomes

List the available outcomes for the node type.

Usage:

```
am> action TimerStop --realm Realm --body body --actionName listOutcomes
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "title" : "Some configuration of the node. This does not need to be complete against the
 configuration schema."
}
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action TimerStop --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query TimerStop --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read TimerStop --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update TimerStop --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "startTimeProperty" : {
      "title" : "Start Time Property",
      "description" : "Identifier of property in which start time should have been stored by a \"Timer
 Start\" node.",
      "propertyOrder" : 100,
      "type" : "string",
      "exampleValue" : ""
    },
    "metricKey" : {
      "title" : "Metric Key",
      "description" : "Identifier of metric to update when this node is processed.",
      "propertyOrder" : 200,
      "type" : "string",
      "exampleValue" : ""
    }
  },
  "required" : [ "metricKey", "startTimeProperty" ]
}
```

TivoliDirectoryServer

Realm Operations

Resource path: `/realm-config/services/id-repositories/LDAPv3ForTivoli`

Resource version: `1.0`

create

Usage:

```
am> create TivoliDirectoryServer --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "userconfig" : {
      "type" : "object",
      "title" : "User Configuration",
      "propertyOrder" : 3,
      "properties" : {
        "sun-idrepo-ldapv3-config-isactive" : {
          "title" : "Attribute Name of User Status",
          "description" : "",
          "propertyOrder" : 2600,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-users-search-filter" : {
          "title" : "LDAP Users  Search Filter",
          "description" : "",
          "propertyOrder" : 2200,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-inactive" : {
          "title" : "User Status Inactive Value",
          "description" : "",
          "propertyOrder" : 2800,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-auth-kba-attr" : {
          "title" : "Knowledge Based Authentication Attribute Name",
          "description" : "",
          "propertyOrder" : 5300,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-user-attributes" : {
          "title" : "LDAP User Attributes",
          "description" : "",
```

```
          "propertyOrder" : 2400,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-auth-kba-attempts-attr" : {
          "title" : "Knowledge Based Authentication Attempts Attribute Name",
          "description" : "",
          "propertyOrder" : 5340,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-users-search-attribute" : {
          "title" : "LDAP Users  Search Attribute",
          "description" : "",
          "propertyOrder" : 2100,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-auth-kba-index-attr" : {
          "title" : "Knowledge Based Authentication Active Index",
          "description" : "",
          "propertyOrder" : 5400,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-people-container-name" : {
          "title" : "LDAP People Container Naming Attribute",
          "description" : "",
          "propertyOrder" : 5000,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-user-objectclass" : {
          "title" : "LDAP User Object Class",
          "description" : "",
          "propertyOrder" : 2300,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-createuser-attr-mapping" : {
          "title" : "Create User Attribute Mapping",
```

```
        "description" : "Format: attribute name or TargetAttributeName=SourceAttributeName",
        "propertyOrder" : 2500,
        "required" : false,
        "items" : {
          "type" : "string"
        },
        "type" : "array",
        "exampleValue" : ""
      },
      "sun-idrepo-ldapv3-config-people-container-value" : {
        "title" : "LDAP People Container Value",
        "description" : "",
        "propertyOrder" : 5100,
        "required" : false,
        "type" : "string",
        "exampleValue" : ""
      },
      "sun-idrepo-ldapv3-config-active" : {
        "title" : "User Status Active Value",
        "description" : "",
        "propertyOrder" : 2700,
        "required" : false,
        "type" : "string",
        "exampleValue" : ""
      }
    }
  },
  "groupconfig" : {
    "type" : "object",
    "title" : "Group Configuration",
    "propertyOrder" : 5,
    "properties" : {
      "sun-idrepo-ldapv3-config-memberof" : {
        "title" : "Attribute Name for Group Membership",
        "description" : "",
        "propertyOrder" : 3500,
        "required" : false,
        "type" : "string",
        "exampleValue" : ""
      },
      "sun-idrepo-ldapv3-config-group-container-value" : {
        "title" : "LDAP Groups Container Value",
        "description" : "",
        "propertyOrder" : 3200,
        "required" : false,
        "type" : "string",
        "exampleValue" : ""
      },
      "sun-idrepo-ldapv3-config-group-objectclass" : {
        "title" : "LDAP Groups Object Class",
        "description" : "",
        "propertyOrder" : 3300,
        "required" : false,
        "items" : {
          "type" : "string"
        },
        "type" : "array",
        "exampleValue" : ""
      },
```

```
        "sun-idrepo-ldapv3-config-groups-search-filter" : {
          "title" : "LDAP Groups Search Filter",
          "description" : "",
          "propertyOrder" : 3000,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-uniquemember" : {
          "title" : "Attribute Name of Unique Member",
          "description" : "",
          "propertyOrder" : 3600,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-dftgroupmember" : {
          "title" : "Default Group Member's User DN",
          "description" : "User automatically added when group is created.",
          "propertyOrder" : 3800,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-group-attributes" : {
          "title" : "LDAP Groups Attributes",
          "description" : "",
          "propertyOrder" : 3400,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-group-container-name" : {
          "title" : "LDAP Groups Container Naming Attribute",
          "description" : "",
          "propertyOrder" : 3100,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-groups-search-attribute" : {
          "title" : "LDAP Groups Search Attribute",
          "description" : "",
          "propertyOrder" : 2900,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "cachecontrol" : {
      "type" : "object",
      "title" : "Cache Control",
      "propertyOrder" : 9,
      "properties" : {
        "sun-idrepo-ldapv3-dncache-size" : {
```

```
          "title" : "DN Cache Size",
          "description" : "In DN items, only used when DN Cache is enabled.",
          "propertyOrder" : 6000,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-dncache-enabled" : {
          "title" : "DN Cache",
          "description" : "Used to enable/disable the DN Cache within the OpenAM repository
implementation.<br><br>The DN Cache is used to cache DN lookups which tend to happen in bursts during
authentication. The DN Cache can become out of date when a user is moved or renamed in the underlying
LDAP store and this is not reflected in a persistent search result. Enable when the underlying LDAP
store supports persistent search and move/rename (mod_dn) results are available.",
          "propertyOrder" : 5900,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        }
      }
    },
    "ldapsettings" : {
      "type" : "object",
      "title" : "Server Settings",
      "propertyOrder" : 0,
      "properties" : {
        "openam-idrepo-ldapv3-heartbeat-timeunit" : {
          "title" : "LDAP Connection Heartbeat Time Unit",
          "description" : "Defines the time unit corresponding to the Heartbeat Interval
setting.<br><br>This setting controls how often OpenAM <b>should</b> send a heartbeat search request
to the configured directory. If a connection becomes unresponsive (e.g. due to a network error) then
it may take up to the interval period before the problem is detected. Use along with the Heartbeat
Interval parameter to define the exact interval.",
          "propertyOrder" : 1400,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-organization_name" : {
          "title" : "LDAP Organization DN",
          "description" : "",
          "propertyOrder" : 900,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "openam-idrepo-ldapv3-affinity-enabled" : {
          "title" : "Affinity Enabled",
          "description" : "Enables affinity based request load balancing when accessing the user store
servers (based on DN). It is imperative that the connection string setting is set to the same value
for all OpenAM servers in the deployment when this feature is enabled.",
          "propertyOrder" : 6200,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-connection-mode" : {
          "title" : "LDAP Connection Mode",
```

```
          "description" : "Defines which protocol/operation is used to establish the connection to
the LDAP Directory Server.<br><br>If 'LDAP' is selected, the connection <b>won't be secured</b> and
passwords are transferred in <b>cleartext</b> over the network.<br/> If 'LDAPS' is selected, the
connection is secured via SSL or TLS. <br/> If 'StartTLS' is selected, the connection is secured by
using StartTLS extended operation.",
          "propertyOrder" : 1000,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-authpw" : {
          "title" : "LDAP Bind Password",
          "description" : "",
          "propertyOrder" : 800,
          "required" : false,
          "type" : "string",
          "format" : "password",
          "exampleValue" : ""
        },
        "openam-idrepo-ldapv3-behera-support-enabled" : {
          "title" : "Behera Support Enabled",
          "description" : "When enabled, Behera draft control will be used in the outgoing requests
for operations that may modify password value. This will allow OpenAM to display password policy
related error messages when password policies are not met.",
          "propertyOrder" : 6100,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "openam-idrepo-ldapv3-heartbeat-interval" : {
          "title" : "LDAP Connection Heartbeat Interval",
          "description" : "Specifies how often should OpenAM send a heartbeat request to the
directory.<br><br>This setting controls how often OpenAM <b>should</b> send a heartbeat search
request to the configured directory. If a connection becomes unresponsive (e.g. due to a network
error) then it may take up to the interval period before the problem is detected. Use along with the
Heartbeat Time Unit parameter to define the exact interval. Zero or negative value will result in
disabling heartbeat requests.",
          "propertyOrder" : 1300,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-authid" : {
          "title" : "LDAP Bind DN",
          "description" : "A user or admin with sufficient access rights to perform the supported
operations.",
          "propertyOrder" : 700,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-search-scope" : {
          "title" : "LDAPv3 Plug-in Search Scope",
          "description" : "",
          "propertyOrder" : 2000,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
```

```
        "sun-idrepo-ldapv3-config-max-result" : {
          "title" : "Maximum Results Returned from Search",
          "description" : "",
          "propertyOrder" : 1500,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-connection_pool_max_size" : {
          "title" : "LDAP Connection Pool Maximum Size",
          "description" : "",
          "propertyOrder" : 1200,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-ldap-server" : {
          "title" : "LDAP Server",
          "description" : "Format: LDAP server host name:port | server_ID | site_ID",
          "propertyOrder" : 600,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "minItems" : 1,
          "type" : "array",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-time-limit" : {
          "title" : "Search Timeout",
          "description" : "In seconds.",
          "propertyOrder" : 1600,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-connection_pool_min_size" : {
          "title" : "LDAP Connection Pool Minimum Size",
          "description" : "",
          "propertyOrder" : 1100,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        }
      }
    },
    "persistentsearch" : {
      "type" : "object",
      "title" : "Persistent Search Controls",
      "propertyOrder" : 7,
      "properties" : {
        "sun-idrepo-ldapv3-config-psearch-filter" : {
          "title" : "Persistent Search Filter",
          "description" : "",
          "propertyOrder" : 5600,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
```

```
        "sun-idrepo-ldapv3-config-psearchbase" : {
          "title" : "Persistent Search Base DN",
          "description" : "",
          "propertyOrder" : 5500,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-psearch-scope" : {
          "title" : "Persistent Search Scope",
          "description" : "",
          "propertyOrder" : 5700,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "pluginconfig" : {
      "type" : "object",
      "title" : "Plug-in Configuration",
      "propertyOrder" : 2,
      "properties" : {
        "sunIdRepoAttributeMapping" : {
          "title" : "Attribute Name Mapping",
          "description" : "",
          "propertyOrder" : 1800,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "sunIdRepoClass" : {
          "title" : "LDAPv3 Repository Plug-in Class Name",
          "description" : "",
          "propertyOrder" : 1700,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "sunIdRepoSupportedOperations" : {
          "title" : "LDAPv3 Plug-in Supported Types and Operations",
          "description" : "",
          "propertyOrder" : 1900,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        }
      }
    },
    "authentication" : {
      "type" : "object",
      "title" : "Authentication Configuration",
      "propertyOrder" : 4,
```

```
      "properties" : {
        "sun-idrepo-ldapv3-config-auth-naming-attr" : {
          "title" : "Authentication Naming Attribute",
          "description" : "",
          "propertyOrder" : 5200,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "errorhandling" : {
      "type" : "object",
      "title" : "Error Handling Configuration",
      "propertyOrder" : 8,
      "properties" : {
        "com.iplanet.am.ldap.connection.delay.between.retries" : {
          "title" : "The Delay Time Between Retries",
          "description" : "In milliseconds.",
          "propertyOrder" : 5800,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        }
      }
    }
  }
}
```

delete

Usage:

```
am> delete TivoliDirectoryServer --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action TivoliDirectoryServer --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action TivoliDirectoryServer --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action TivoliDirectoryServer --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query TivoliDirectoryServer --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read TivoliDirectoryServer --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update TivoliDirectoryServer --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "userconfig" : {
      "type" : "object",
      "title" : "User Configuration",
      "propertyOrder" : 3,
      "properties" : {
        "sun-idrepo-ldapv3-config-isactive" : {
          "title" : "Attribute Name of User Status",
          "description" : "",
          "propertyOrder" : 2600,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-users-search-filter" : {
          "title" : "LDAP Users  Search Filter",
          "description" : "",
          "propertyOrder" : 2200,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-inactive" : {
          "title" : "User Status Inactive Value",
          "description" : "",
          "propertyOrder" : 2800,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-auth-kba-attr" : {
          "title" : "Knowledge Based Authentication Attribute Name",
          "description" : "",
          "propertyOrder" : 5300,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-user-attributes" : {
          "title" : "LDAP User Attributes",
          "description" : "",
          "propertyOrder" : 2400,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-auth-kba-attempts-attr" : {
```

```
          "title" : "Knowledge Based Authentication Attempts Attribute Name",
          "description" : "",
          "propertyOrder" : 5340,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-users-search-attribute" : {
          "title" : "LDAP Users  Search Attribute",
          "description" : "",
          "propertyOrder" : 2100,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-auth-kba-index-attr" : {
          "title" : "Knowledge Based Authentication Active Index",
          "description" : "",
          "propertyOrder" : 5400,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-people-container-name" : {
          "title" : "LDAP People Container Naming Attribute",
          "description" : "",
          "propertyOrder" : 5000,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-user-objectclass" : {
          "title" : "LDAP User Object Class",
          "description" : "",
          "propertyOrder" : 2300,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-createuser-attr-mapping" : {
          "title" : "Create User Attribute Mapping",
          "description" : "Format: attribute name or TargetAttributeName=SourceAttributeName",
          "propertyOrder" : 2500,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
```

```
        "sun-idrepo-ldapv3-config-people-container-value" : {
          "title" : "LDAP People Container Value",
          "description" : "",
          "propertyOrder" : 5100,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-active" : {
          "title" : "User Status Active Value",
          "description" : "",
          "propertyOrder" : 2700,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "groupconfig" : {
      "type" : "object",
      "title" : "Group Configuration",
      "propertyOrder" : 5,
      "properties" : {
        "sun-idrepo-ldapv3-config-memberof" : {
          "title" : "Attribute Name for Group Membership",
          "description" : "",
          "propertyOrder" : 3500,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-group-container-value" : {
          "title" : "LDAP Groups Container Value",
          "description" : "",
          "propertyOrder" : 3200,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-group-objectclass" : {
          "title" : "LDAP Groups Object Class",
          "description" : "",
          "propertyOrder" : 3300,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-groups-search-filter" : {
          "title" : "LDAP Groups Search Filter",
          "description" : "",
          "propertyOrder" : 3000,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-uniquemember" : {
```

```
          "title" : "Attribute Name of Unique Member",
          "description" : "",
          "propertyOrder" : 3600,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-dftgroupmember" : {
          "title" : "Default Group Member's User DN",
          "description" : "User automatically added when group is created.",
          "propertyOrder" : 3800,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-group-attributes" : {
          "title" : "LDAP Groups Attributes",
          "description" : "",
          "propertyOrder" : 3400,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-group-container-name" : {
          "title" : "LDAP Groups Container Naming Attribute",
          "description" : "",
          "propertyOrder" : 3100,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-groups-search-attribute" : {
          "title" : "LDAP Groups Search Attribute",
          "description" : "",
          "propertyOrder" : 2900,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "cachecontrol" : {
      "type" : "object",
      "title" : "Cache Control",
      "propertyOrder" : 9,
      "properties" : {
        "sun-idrepo-ldapv3-dncache-size" : {
          "title" : "DN Cache Size",
          "description" : "In DN items, only used when DN Cache is enabled.",
          "propertyOrder" : 6000,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-dncache-enabled" : {
          "title" : "DN Cache",
```

```
          "description" : "Used to enable/disable the DN Cache within the OpenAM repository
implementation.<br><br>The DN Cache is used to cache DN lookups which tend to happen in bursts during
authentication. The DN Cache can become out of date when a user is moved or renamed in the underlying
LDAP store and this is not reflected in a persistent search result. Enable when the underlying LDAP
store supports persistent search and move/rename (mod_dn) results are available.",
          "propertyOrder" : 5900,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        }
      }
    },
    "ldapsettings" : {
      "type" : "object",
      "title" : "Server Settings",
      "propertyOrder" : 0,
      "properties" : {
        "openam-idrepo-ldapv3-heartbeat-timeunit" : {
          "title" : "LDAP Connection Heartbeat Time Unit",
          "description" : "Defines the time unit corresponding to the Heartbeat Interval
setting.<br><br>This setting controls how often OpenAM <b>should</b> send a heartbeat search request
to the configured directory. If a connection becomes unresponsive (e.g. due to a network error) then
it may take up to the interval period before the problem is detected. Use along with the Heartbeat
Interval parameter to define the exact interval.",
          "propertyOrder" : 1400,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-organization_name" : {
          "title" : "LDAP Organization DN",
          "description" : "",
          "propertyOrder" : 900,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "openam-idrepo-ldapv3-affinity-enabled" : {
          "title" : "Affinity Enabled",
          "description" : "Enables affinity based request load balancing when accessing the user store
servers (based on DN). It is imperative that the connection string setting is set to the same value
for all OpenAM servers in the deployment when this feature is enabled.",
          "propertyOrder" : 6200,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-connection-mode" : {
          "title" : "LDAP Connection Mode",
          "description" : "Defines which protocol/operation is used to establish the connection to
the LDAP Directory Server.<br><br>If 'LDAP' is selected, the connection <b>won't be secured</b> and
passwords are transferred in <b>cleartext</b> over the network.<br/> If 'LDAPS' is selected, the
connection is secured via SSL or TLS. <br/> If 'StartTLS' is selected, the connection is secured by
using StartTLS extended operation.",
          "propertyOrder" : 1000,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
```

```
       "sun-idrepo-ldapv3-config-authpw" : {
         "title" : "LDAP Bind Password",
         "description" : "",
         "propertyOrder" : 800,
         "required" : false,
         "type" : "string",
         "format" : "password",
         "exampleValue" : ""
       },
       "openam-idrepo-ldapv3-behera-support-enabled" : {
         "title" : "Behera Support Enabled",
         "description" : "When enabled, Behera draft control will be used in the outgoing requests
for operations that may modify password value. This will allow OpenAM to display password policy
related error messages when password policies are not met.",
         "propertyOrder" : 6100,
         "required" : false,
         "type" : "boolean",
         "exampleValue" : ""
       },
       "openam-idrepo-ldapv3-heartbeat-interval" : {
         "title" : "LDAP Connection Heartbeat Interval",
         "description" : "Specifies how often should OpenAM send a heartbeat request to the
directory.<br><br>This setting controls how often OpenAM <b>should</b> send a heartbeat search
request to the configured directory. If a connection becomes unresponsive (e.g. due to a network
error) then it may take up to the interval period before the problem is detected. Use along with the
Heartbeat Time Unit parameter to define the exact interval. Zero or negative value will result in
disabling heartbeat requests.",
         "propertyOrder" : 1300,
         "required" : false,
         "type" : "integer",
         "exampleValue" : ""
       },
       "sun-idrepo-ldapv3-config-authid" : {
         "title" : "LDAP Bind DN",
         "description" : "A user or admin with sufficient access rights to perform the supported
operations.",
         "propertyOrder" : 700,
         "required" : false,
         "type" : "string",
         "exampleValue" : ""
       },
       "sun-idrepo-ldapv3-config-search-scope" : {
         "title" : "LDAPv3 Plug-in Search Scope",
         "description" : "",
         "propertyOrder" : 2000,
         "required" : false,
         "type" : "string",
         "exampleValue" : ""
       },
       "sun-idrepo-ldapv3-config-max-result" : {
         "title" : "Maximum Results Returned from Search",
         "description" : "",
         "propertyOrder" : 1500,
         "required" : false,
         "type" : "integer",
         "exampleValue" : ""
       },
       "sun-idrepo-ldapv3-config-connection_pool_max_size" : {
         "title" : "LDAP Connection Pool Maximum Size",
```

```
          "description" : "",
          "propertyOrder" : 1200,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-ldap-server" : {
          "title" : "LDAP Server",
          "description" : "Format: LDAP server host name:port | server_ID | site_ID",
          "propertyOrder" : 600,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "minItems" : 1,
          "type" : "array",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-time-limit" : {
          "title" : "Search Timeout",
          "description" : "In seconds.",
          "propertyOrder" : 1600,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-connection_pool_min_size" : {
          "title" : "LDAP Connection Pool Minimum Size",
          "description" : "",
          "propertyOrder" : 1100,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        }
      }
    },
    "persistentsearch" : {
      "type" : "object",
      "title" : "Persistent Search Controls",
      "propertyOrder" : 7,
      "properties" : {
        "sun-idrepo-ldapv3-config-psearch-filter" : {
          "title" : "Persistent Search Filter",
          "description" : "",
          "propertyOrder" : 5600,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-psearchbase" : {
          "title" : "Persistent Search Base DN",
          "description" : "",
          "propertyOrder" : 5500,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "sun-idrepo-ldapv3-config-psearch-scope" : {
          "title" : "Persistent Search Scope",
```

```
        "description" : "",
        "propertyOrder" : 5700,
        "required" : false,
        "type" : "string",
        "exampleValue" : ""
      }
    }
  },
  "pluginconfig" : {
    "type" : "object",
    "title" : "Plug-in Configuration",
    "propertyOrder" : 2,
    "properties" : {
      "sunIdRepoAttributeMapping" : {
        "title" : "Attribute Name Mapping",
        "description" : "",
        "propertyOrder" : 1800,
        "required" : false,
        "items" : {
          "type" : "string"
        },
        "type" : "array",
        "exampleValue" : ""
      },
      "sunIdRepoClass" : {
        "title" : "LDAPv3 Repository Plug-in Class Name",
        "description" : "",
        "propertyOrder" : 1700,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
      },
      "sunIdRepoSupportedOperations" : {
        "title" : "LDAPv3 Plug-in Supported Types and Operations",
        "description" : "",
        "propertyOrder" : 1900,
        "required" : false,
        "items" : {
          "type" : "string"
        },
        "type" : "array",
        "exampleValue" : ""
      }
    }
  },
  "authentication" : {
    "type" : "object",
    "title" : "Authentication Configuration",
    "propertyOrder" : 4,
    "properties" : {
      "sun-idrepo-ldapv3-config-auth-naming-attr" : {
        "title" : "Authentication Naming Attribute",
        "description" : "",
        "propertyOrder" : 5200,
        "required" : false,
        "type" : "string",
        "exampleValue" : ""
      }
    }
```

```
    },
    "errorhandling" : {
      "type" : "object",
      "title" : "Error Handling Configuration",
      "propertyOrder" : 8,
      "properties" : {
        "com.iplanet.am.ldap.connection.delay.between.retries" : {
          "title" : "The Delay Time Between Retries",
          "description" : "In milliseconds.",
          "propertyOrder" : 5800,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        }
      }
    }
  }
}
```

TransactionAuthentication

Realm Operations

Resource path: `/realm-config/services/transaction`

Resource version: `1.0`

create

Usage:

```
am> create TransactionAuthentication --realm Realm --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "timeToLive" : {
      "title" : "Time to Live",
      "description" : "The number of seconds within which the transaction must be completed.",
      "propertyOrder" : 0,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
```

delete

Usage:

```
am> delete TransactionAuthentication --realm Realm
```

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action TransactionAuthentication --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action TransactionAuthentication --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action TransactionAuthentication --realm Realm --actionName nextdescendents
```

read

Usage:

```
am> read TransactionAuthentication --realm Realm
```

update

Usage:

```
am> update TransactionAuthentication --realm Realm --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "timeToLive" : {
      "title" : "Time to Live",
      "description" : "The number of seconds within which the transaction must be completed.",
      "propertyOrder" : 0,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
```

Global Operations

Resource path: `/global-config/services/transaction`

Resource version: `1.0`

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action TransactionAuthentication --global --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action TransactionAuthentication --global --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action TransactionAuthentication --global --actionName nextdescendents
```

read

Usage:

```
am> read TransactionAuthentication --global
```

update

Usage:

```
am> update TransactionAuthentication --global --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "defaults" : {
      "properties" : {
        "timeToLive" : {
          "title" : "Time to Live",
          "description" : "The number of seconds within which the transaction must be completed.",
          "propertyOrder" : 0,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      },
      "type" : "object",
      "title" : "Realm Defaults"
    }
  }
}
```

TrustedJwtIssuer

Realm Operations

Agents handler that is responsible for managing agents

Resource path: `/realm-config/agents/TrustedJwtIssuer`

Resource version: `1.0`

create

Usage:

```
am> create TrustedJwtIssuer --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "agentgroup" : {
      "title" : "Group",
      "description" : "Add the agent to a group to allow inheritance of property values from the
 group. <br>Changing the group will update inherited property values. <br>Inherited property values
 are copied to the agent.",
      "propertyOrder" : 5,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
    },
    "jwksUri" : {
      "title" : "JWKs URI",
      "description" : "URI to retrieve JWK verification keys from to validate the JWT signature.",
      "propertyOrder" : 20,
      "type" : "object",
      "exampleValue" : "",
      "properties" : {
        "inherited" : {
          "type" : "boolean",
          "required" : true
        },
        "value" : {
          "type" : "string",
          "required" : false
        }
      }
    },
    "issuer" : {
      "title" : "JWT Issuer",
      "description" : "Expected 'iss' claim identifier for this JWT issuer.",
      "propertyOrder" : 10,
      "type" : "object",
      "exampleValue" : "",
      "properties" : {
        "inherited" : {
```

```
          "type" : "boolean",
          "required" : true
        },
        "value" : {
          "type" : "string",
          "required" : true
        }
      }
    },
    "allowedSubjects" : {
      "title" : "Allowed Subjects",
      "description" : "List of subjects which this provider is allowed to provide consent for. If
blank then the provider can provide consent for any user in this realm.",
      "propertyOrder" : 60,
      "items" : {
        "type" : "string"
      },
      "type" : "object",
      "exampleValue" : "",
      "properties" : {
        "inherited" : {
          "type" : "boolean",
          "required" : true
        },
        "value" : {
          "type" : "array",
          "required" : false
        }
      }
    },
    "resourceOwnerIdentityClaim" : {
      "title" : "Resource Owner Identity Claim",
      "description" : "Claim in the JWT that identifies the resource owner account in AM. Defaults to
\"sub\".",
      "propertyOrder" : 50,
      "type" : "object",
      "exampleValue" : "",
      "properties" : {
        "inherited" : {
          "type" : "boolean",
          "required" : true
        },
        "value" : {
          "type" : "string",
          "required" : false
        }
      }
    },
    "jwksCacheTimeout" : {
      "title" : "JWKs URI content cache timeout in ms",
      "description" : "To avoid loading the JWKS URI content for every operation, the JWKS content is
cached. This timeout defines the maximum amount of time the JWKS URI content can be cached before
being refreshed.",
      "propertyOrder" : 70,
      "type" : "object",
      "exampleValue" : "",
      "properties" : {
        "inherited" : {
          "type" : "boolean",
```

```
          "required" : true
        },
        "value" : {
          "type" : "integer",
          "required" : false
        }
      }
    },
    "jwkSet" : {
      "title" : "JWK Set",
      "description" : "Manually entered JWK Set of verification keys to validate the JWT signature.",
      "propertyOrder" : 30,
      "type" : "object",
      "exampleValue" : "",
      "properties" : {
        "inherited" : {
          "type" : "boolean",
          "required" : true
        },
        "value" : {
          "type" : "string",
          "required" : false
        }
      }
    },
    "consentedScopesClaim" : {
      "title" : "Consented Scopes Claim",
      "description" : "Optional claim within the JWT that lists the scopes that the user has consented
to. The scopes can be represented either as a JSON array of strings, or as a single space-separated
string.",
      "propertyOrder" : 40,
      "type" : "object",
      "exampleValue" : "",
      "properties" : {
        "inherited" : {
          "type" : "boolean",
          "required" : true
        },
        "value" : {
          "type" : "string",
          "required" : false
        }
      }
    },
    "jwkStoreCacheMissCacheTime" : {
      "title" : "JWKs URI content cache miss cache time",
      "description" : "To avoid loading the JWKS URI content for every operation, especially when
the kid is not in the jwks content already cached, the JWKS content will be cached for a minimum
period of time. This cache miss cache time defines the minimum amount of time the JWKS URI content is
cached.",
      "propertyOrder" : 80,
      "type" : "object",
      "exampleValue" : "",
      "properties" : {
        "inherited" : {
          "type" : "boolean",
          "required" : true
        },
        "value" : {
```

```
          "type" : "integer",
          "required" : false
        }
      }
    }
  }
}
```

delete

Usage:

```
am> delete TrustedJwtIssuer --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action TrustedJwtIssuer --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action TrustedJwtIssuer --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action TrustedJwtIssuer --realm Realm --actionName nextdescendents
```

query

Querying the agents of a specific type

Usage:

```
am> query TrustedJwtIssuer --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read TrustedJwtIssuer --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update TrustedJwtIssuer --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "agentgroup" : {
      "title" : "Group",
      "description" : "Add the agent to a group to allow inheritance of property values from the
 group. <br>Changing the group will update inherited property values. <br>Inherited property values
 are copied to the agent.",
      "propertyOrder" : 5,
      "required" : false,
      "type" : "string",
      "exampleValue" : ""
    },
    "jwksUri" : {
      "title" : "JWKs URI",
      "description" : "URI to retrieve JWK verification keys from to validate the JWT signature.",
      "propertyOrder" : 20,
```

```
      "type" : "object",
      "exampleValue" : "",
      "properties" : {
        "inherited" : {
          "type" : "boolean",
          "required" : true
        },
        "value" : {
          "type" : "string",
          "required" : false
        }
      }
    },
    "issuer" : {
      "title" : "JWT Issuer",
      "description" : "Expected 'iss' claim identifier for this JWT issuer.",
      "propertyOrder" : 10,
      "type" : "object",
      "exampleValue" : "",
      "properties" : {
        "inherited" : {
          "type" : "boolean",
          "required" : true
        },
        "value" : {
          "type" : "string",
          "required" : true
        }
      }
    },
    "allowedSubjects" : {
      "title" : "Allowed Subjects",
      "description" : "List of subjects which this provider is allowed to provide consent for. If
blank then the provider can provide consent for any user in this realm.",
      "propertyOrder" : 60,
      "items" : {
        "type" : "string"
      },
      "type" : "object",
      "exampleValue" : "",
      "properties" : {
        "inherited" : {
          "type" : "boolean",
          "required" : true
        },
        "value" : {
          "type" : "array",
          "required" : false
        }
      }
    },
    "resourceOwnerIdentityClaim" : {
      "title" : "Resource Owner Identity Claim",
      "description" : "Claim in the JWT that identifies the resource owner account in AM. Defaults to
\"sub\".",
      "propertyOrder" : 50,
      "type" : "object",
      "exampleValue" : "",
      "properties" : {
```

```
        "inherited" : {
          "type" : "boolean",
          "required" : true
        },
        "value" : {
          "type" : "string",
          "required" : false
        }
      }
    },
    "jwksCacheTimeout" : {
      "title" : "JWKs URI content cache timeout in ms",
      "description" : "To avoid loading the JWKS URI content for every operation, the JWKS content is
cached. This timeout defines the maximum amount of time the JWKS URI content can be cached before
being refreshed.",
      "propertyOrder" : 70,
      "type" : "object",
      "exampleValue" : "",
      "properties" : {
        "inherited" : {
          "type" : "boolean",
          "required" : true
        },
        "value" : {
          "type" : "integer",
          "required" : false
        }
      }
    },
    "jwkSet" : {
      "title" : "JWK Set",
      "description" : "Manually entered JWK Set of verification keys to validate the JWT signature.",
      "propertyOrder" : 30,
      "type" : "object",
      "exampleValue" : "",
      "properties" : {
        "inherited" : {
          "type" : "boolean",
          "required" : true
        },
        "value" : {
          "type" : "string",
          "required" : false
        }
      }
    },
    "consentedScopesClaim" : {
      "title" : "Consented Scopes Claim",
      "description" : "Optional claim within the JWT that lists the scopes that the user has consented
to. The scopes can be represented either as a JSON array of strings, or as a single space-separated
string.",
      "propertyOrder" : 40,
      "type" : "object",
      "exampleValue" : "",
      "properties" : {
        "inherited" : {
          "type" : "boolean",
          "required" : true
        },
```

```
        "value" : {
          "type" : "string",
          "required" : false
        }
      }
    },
    "jwkStoreCacheMissCacheTime" : {
      "title" : "JWKs URI content cache miss cache time",
      "description" : "To avoid loading the JWKS URI content for every operation, especially when
 the kid is not in the jwks content already cached, the JWKS content will be cached for a minimum
 period of time. This cache miss cache time defines the minimum amount of time the JWKS URI content is
 cached.",
      "propertyOrder" : 80,
      "type" : "object",
      "exampleValue" : "",
      "properties" : {
        "inherited" : {
          "type" : "boolean",
          "required" : true
        },
        "value" : {
          "type" : "integer",
          "required" : false
        }
      }
    }
  }
}
```


TrustedUserDevices

Realm Operations

Trusted devices service is responsible for querying and deleting trusted devices.

Resource path: `/users/{user}/devices/trusted`

Resource version: `1.0`

delete

Delete trusted user device

Usage:

```
am> delete TrustedUserDevices --realm Realm --id id --user user
```

Parameters:

--id

The unique identifier for the resource.

--user

Trusted devices service is responsible for querying and deleting trusted devices.

query

Query trusted user devices

Usage:

```
am> query TrustedUserDevices --realm Realm --filter filter --user user
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all. Fields that can be queried: [*]

--user

Trusted devices service is responsible for querying and deleting trusted devices.

TwitterClient

Realm Operations

Resource path: `/realm-config/services/SocialIdentityProviders/twitterConfig`

Resource version: `1.0`

create

Usage:

```
am> create TwitterClient --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
```

```
    "redirectURI" : {
      "title" : "Redirect URL",
      "description" : "",
      "propertyOrder" : 700,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "authenticationIdKey" : {
      "title" : "Auth ID Key",
      "description" : "Field used to identify a user by the social provider.",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "exampleValue" : "sub"
    },
    "clientId" : {
      "title" : "Client ID",
      "description" : "OAuth client_id parameter<p> For more information on the OAuth client_id
parameter refer to the RFC 6749 (http://tools.ietf.org/html/rfc6749#section-2.3.1), section 2.3.1.",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "uiConfig" : {
      "title" : "UI Config Properties",
      "description" : "Mapping of display properties to be defined and consumed by the UI.",
      "propertyOrder" : 9999,
      "required" : true,
      "patternProperties" : {
        ".*" : {
          "type" : "string"
        }
      },
      "type" : "object",
      "exampleValue" : ""
    },
    "requestTokenEndpoint" : {
      "title" : "Request Token Endpoint",
      "description" : "The endpoint for obtaining an access token.",
      "propertyOrder" : 800,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "clientSecret" : {
      "title" : "Client Secret",
      "description" : "OAuth client_secret parameter <p>For more information on the OAuth client_id
parameter refer to the RFC 6749 (http://tools.ietf.org/html/rfc6749#section-2.3.1), section 2.3.1.",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "string",
      "format" : "password",
      "exampleValue" : ""
    },
    "userInfoEndpoint" : {
      "title" : "User Profile Service URL",
```

```
      "description" : "User profile information URL <p> This URL endpoint provides user profile
 information and is provided by the OAuth Identity Provider NB This URL should return JSON objects in
 response.",
      "propertyOrder" : 600,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "transform" : {
      "title" : "Transform Script",
      "description" : "A script that takes the raw profile object as input and outputs the normalized
 profile object.",
      "propertyOrder" : 10000,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "enabled" : {
      "title" : "Enabled",
      "description" : "",
      "propertyOrder" : 1,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "tokenEndpoint" : {
      "title" : "Access Token Endpoint URL",
      "description" : "OAuth access token endpoint URL This is the URL endpoint for access token
 retrieval provided by the OAuth Identity Provider.Refer to the RFC 6749 (http://tools.ietf.org/html/
rfc6749#section-3.2), section 3.2.",
      "propertyOrder" : 500,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "authorizationEndpoint" : {
      "title" : "Authentication Endpoint URL",
      "description" : "OAuth authentication endpoint URL <p> This is the URL endpoint for OAuth
 authentication provided by the OAuth Identity Provider.",
      "propertyOrder" : 400,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
```


delete

Usage:

```
am> delete TwitterClient --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action TwitterClient --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action TwitterClient --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action TwitterClient --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query TwitterClient --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read TwitterClient --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update TwitterClient --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "redirectURI" : {
      "title" : "Redirect URL",
      "description" : "",
      "propertyOrder" : 700,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "authenticationIdKey" : {
      "title" : "Auth ID Key",
      "description" : "Field used to identify a user by the social provider.",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "exampleValue" : "sub"
    },
    "clientId" : {
      "title" : "Client ID",
      "description" : "OAuth client_id parameter<p> For more information on the OAuth client_id
 parameter refer to the RFC 6749 (http://tools.ietf.org/html/rfc6749#section-2.3.1), section 2.3.1.",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "uiConfig" : {
      "title" : "UI Config Properties",
      "description" : "Mapping of display properties to be defined and consumed by the UI.",
      "propertyOrder" : 9999,
      "required" : true,
      "patternProperties" : {
        ".*" : {
          "type" : "string"
```

```
        }
      },
      "type" : "object",
      "exampleValue" : ""
    },
    "requestTokenEndpoint" : {
      "title" : "Request Token Endpoint",
      "description" : "The endpoint for obtaining an access token.",
      "propertyOrder" : 800,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "clientSecret" : {
      "title" : "Client Secret",
      "description" : "OAuth client_secret parameter <p>For more information on the OAuth client_id
 parameter refer to the RFC 6749 (http://tools.ietf.org/html/rfc6749#section-2.3.1), section 2.3.1.",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "string",
      "format" : "password",
      "exampleValue" : ""
    },
    "userInfoEndpoint" : {
      "title" : "User Profile Service URL",
      "description" : "User profile information URL <p> This URL endpoint provides user profile
 information and is provided by the OAuth Identity Provider NB This URL should return JSON objects in
 response.",
      "propertyOrder" : 600,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "transform" : {
      "title" : "Transform Script",
      "description" : "A script that takes the raw profile object as input and outputs the normalized
 profile object.",
      "propertyOrder" : 10000,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "enabled" : {
      "title" : "Enabled",
      "description" : "",
      "propertyOrder" : 1,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "tokenEndpoint" : {
      "title" : "Access Token Endpoint URL",
      "description" : "OAuth access token endpoint URL This is the URL endpoint for access token
 retrieval provided by the OAuth Identity Provider.Refer to the RFC 6749 (http://tools.ietf.org/html/
rfc6749#section-3.2), section 3.2.",
      "propertyOrder" : 500,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
```

```
    },
    "authorizationEndpoint" : {
      "title" : "Authentication Endpoint URL",
      "description" : "OAuth authentication endpoint URL <p> This is the URL endpoint for OAuth
 authentication provided by the OAuth Identity Provider.",
      "propertyOrder" : 400,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
```

UmaDataStoreProperties

Global Operations

An object of property key-value pairs

Resource path: `/global-config/servers/{serverName}/properties/uma`

Resource version: `1.0`

read

Usage:

```
am> read UmaDataStoreProperties --global --serverName serverName
```

Parameters:

`--serverName`

An object of property key-value pairs

update

Usage:

```
am> update UmaDataStoreProperties --global --serverName serverName --body body
```

Parameters:

`--serverName`

An object of property key-value pairs

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "amconfig.org.forgerock.services.resourcesets.store.common.section" : {
      "title" : "UMA Resource Store",
      "type" : "object",
      "propertyOrder" : 0,
      "properties" : {
        "org.forgerock.services.resourcesets.store.location" : {
          "title" : "Store Mode",
          "type" : "object",
          "propertyOrder" : 0,
          "description" : "",
          "properties" : {
            "value" : {
              "enum" : [ "default", "external" ],
              "options" : {
                "enum_titles" : [ "Default Token Store", "External Token Store" ]
              },
              "type" : "string",
              "required" : false
            },
            "inherited" : {
              "type" : "boolean",
              "required" : true
            }
          }
        },
        "org.forgerock.services.resourcesets.store.root.suffix" : {
          "title" : "Root Suffix",
          "type" : "object",
          "propertyOrder" : 1,
          "description" : "",
          "properties" : {
            "value" : {
              "type" : "string",
              "required" : false
            },
            "inherited" : {
              "type" : "boolean",
              "required" : true
            }
          }
        },
        "org.forgerock.services.resourcesets.store.max.connections" : {
          "title" : "Max Connections",
          "type" : "object",
          "propertyOrder" : 2,
          "description" : "",
          "properties" : {
            "value" : {
              "type" : "string",
              "required" : false
            },
            "inherited" : {
```

```
              "type" : "boolean",
              "required" : true
            }
          }
        }
      }
    },
    "amconfig.org.forgerock.services.resourcesets.store.external.section" : {
      "title" : "External UMA Resource Store Configuration",
      "type" : "object",
      "propertyOrder" : 1,
      "properties" : {
        "org.forgerock.services.resourcesets.store.ssl.enabled" : {
          "title" : "SSL/TLS Enabled",
          "type" : "object",
          "propertyOrder" : 0,
          "description" : "",
          "properties" : {
            "value" : {
              "type" : "boolean",
              "required" : false
            },
            "inherited" : {
              "type" : "boolean",
              "required" : true
            }
          }
        },
        "org.forgerock.services.resourcesets.store.starttls.enabled" : {
          "title" : "Start TLS",
          "type" : "object",
          "propertyOrder" : 1,
          "description" : "Specifies whether to use StartTLS for the connection.",
          "properties" : {
            "value" : {
              "type" : "boolean",
              "required" : false
            },
            "inherited" : {
              "type" : "boolean",
              "required" : true
            }
          }
        },
        "org.forgerock.services.resourcesets.store.directory.name" : {
          "title" : "Connection String(s)",
          "type" : "object",
          "propertyOrder" : 2,
          "description" : "An ordered list of connection strings for LDAP directories. Each connection
 string is composed as follows: <code>HOST:PORT[|SERVERID[|SITEID]]</code>, where server and site
 IDs are optional parameters that will prioritize that connection to use from the specified nodes.
 Multiple connection strings should be comma-separated, e.g. <code>host1:389,host2:50389|server1|
site1,host3:50389</code>.",
          "properties" : {
            "value" : {
              "type" : "string",
              "required" : false
            },
            "inherited" : {
```

```
              "type" : "boolean",
              "required" : true
            }
          }
        },
        "org.forgerock.services.resourcesets.store.loginid" : {
          "title" : "Login Id",
          "type" : "object",
          "propertyOrder" : 3,
          "description" : "",
          "properties" : {
            "value" : {
              "type" : "string",
              "required" : false
            },
            "inherited" : {
              "type" : "boolean",
              "required" : true
            }
          }
        },
        "org.forgerock.services.resourcesets.store.password" : {
          "title" : "Password",
          "type" : "object",
          "propertyOrder" : 4,
          "description" : "",
          "properties" : {
            "value" : {
              "type" : "string",
              "required" : false,
              "format" : "password"
            },
            "inherited" : {
              "type" : "boolean",
              "required" : true
            }
          }
        },
        "org.forgerock.services.resourcesets.store.heartbeat" : {
          "title" : "Heartbeat",
          "type" : "object",
          "propertyOrder" : 5,
          "description" : "",
          "properties" : {
            "value" : {
              "type" : "integer",
              "required" : false
            },
            "inherited" : {
              "type" : "boolean",
              "required" : true
            }
          }
        }
      }
    },
    "amconfig.org.forgerock.services.umaaudit.store.common.section" : {
      "title" : "UMA Audit Store",
      "type" : "object",
```

```
      "propertyOrder" : 2,
      "properties" : {
        "org.forgerock.services.umaaudit.store.location" : {
          "title" : "Store Mode",
          "type" : "object",
          "propertyOrder" : 0,
          "description" : "",
          "properties" : {
            "value" : {
              "enum" : [ "default", "external" ],
              "options" : {
                "enum_titles" : [ "Default Token Store", "External Token Store" ]
              },
              "type" : "string",
              "required" : false
            },
            "inherited" : {
              "type" : "boolean",
              "required" : true
            }
          }
        },
        "org.forgerock.services.umaaudit.store.root.suffix" : {
          "title" : "Root Suffix",
          "type" : "object",
          "propertyOrder" : 1,
          "description" : "",
          "properties" : {
            "value" : {
              "type" : "string",
              "required" : false
            },
            "inherited" : {
              "type" : "boolean",
              "required" : true
            }
          }
        },
        "org.forgerock.services.umaaudit.store.max.connections" : {
          "title" : "Max Connections",
          "type" : "object",
          "propertyOrder" : 2,
          "description" : "",
          "properties" : {
            "value" : {
              "type" : "string",
              "required" : false
            },
            "inherited" : {
              "type" : "boolean",
              "required" : true
            }
          }
        }
      }
    },
    "amconfig.org.forgerock.services.umaaudit.store.external.section" : {
      "title" : "External UMA Audit Store Configuration",
      "type" : "object",
```

```
      "propertyOrder" : 3,
      "properties" : {
        "org.forgerock.services.umaaudit.store.ssl.enabled" : {
          "title" : "SSL/TLS Enabled",
          "type" : "object",
          "propertyOrder" : 0,
          "description" : "",
          "properties" : {
            "value" : {
              "type" : "boolean",
              "required" : false
            },
            "inherited" : {
              "type" : "boolean",
              "required" : true
            }
          }
        },
        "org.forgerock.services.umaaudit.store.starttls.enabled" : {
          "title" : "Start TLS",
          "type" : "object",
          "propertyOrder" : 1,
          "description" : "Specifies whether to use StartTLS for the connection.",
          "properties" : {
            "value" : {
              "type" : "boolean",
              "required" : false
            },
            "inherited" : {
              "type" : "boolean",
              "required" : true
            }
          }
        },
        "org.forgerock.services.umaaudit.store.directory.name" : {
          "title" : "Connection String(s)",
          "type" : "object",
          "propertyOrder" : 2,
          "description" : "An ordered list of connection strings for LDAP directories. Each connection
 string is composed as follows: <code>HOST:PORT[|SERVERID[|SITEID]]</code>, where server and site
 IDs are optional parameters that will prioritize that connection to use from the specified nodes.
 Multiple connection strings should be comma-separated, e.g. <code>host1:389,host2:50389|server1|
site1,host3:50389</code>.",
          "properties" : {
            "value" : {
              "type" : "string",
              "required" : false
            },
            "inherited" : {
              "type" : "boolean",
              "required" : true
            }
          }
        },
        "org.forgerock.services.umaaudit.store.loginid" : {
          "title" : "Login Id",
          "type" : "object",
          "propertyOrder" : 3,
          "description" : "",
```

```
          "properties" : {
            "value" : {
              "type" : "string",
              "required" : false
            },
            "inherited" : {
              "type" : "boolean",
              "required" : true
            }
          }
        },
        "org.forgerock.services.umaaudit.store.password" : {
          "title" : "Password",
          "type" : "object",
          "propertyOrder" : 4,
          "description" : "",
          "properties" : {
            "value" : {
              "type" : "string",
              "required" : false,
              "format" : "password"
            },
            "inherited" : {
              "type" : "boolean",
              "required" : true
            }
          }
        },
        "org.forgerock.services.umaaudit.store.heartbeat" : {
          "title" : "Heartbeat",
          "type" : "object",
          "propertyOrder" : 5,
          "description" : "",
          "properties" : {
            "value" : {
              "type" : "integer",
              "required" : false
            },
            "inherited" : {
              "type" : "boolean",
              "required" : true
            }
          }
        }
      }
    },
    "amconfig.org.forgerock.services.uma.pendingrequests.store.common.section" : {
      "title" : "Pending Requests Store",
      "type" : "object",
      "propertyOrder" : 4,
      "properties" : {
        "org.forgerock.services.uma.pendingrequests.store.location" : {
          "title" : "Store Mode",
          "type" : "object",
          "propertyOrder" : 0,
          "description" : "",
          "properties" : {
            "value" : {
              "enum" : [ "default", "external" ],
```

```
            "options" : {
              "enum_titles" : [ "Default Token Store", "External Token Store" ]
            },
            "type" : "string",
            "required" : false
          },
          "inherited" : {
            "type" : "boolean",
            "required" : true
          }
        }
      },
      "org.forgerock.services.uma.pendingrequests.store.root.suffix" : {
        "title" : "Root Suffix",
        "type" : "object",
        "propertyOrder" : 1,
        "description" : "",
        "properties" : {
          "value" : {
            "type" : "string",
            "required" : false
          },
          "inherited" : {
            "type" : "boolean",
            "required" : true
          }
        }
      },
      "org.forgerock.services.uma.pendingrequests.store.max.connections" : {
        "title" : "Max Connections",
        "type" : "object",
        "propertyOrder" : 2,
        "description" : "",
        "properties" : {
          "value" : {
            "type" : "string",
            "required" : false
          },
          "inherited" : {
            "type" : "boolean",
            "required" : true
          }
        }
      }
    }
  },
  "amconfig.org.forgerock.services.uma.pendingrequests.store.external.section" : {
    "title" : "External Pending Requests Store Configuration",
    "type" : "object",
    "propertyOrder" : 5,
    "properties" : {
      "org.forgerock.services.uma.pendingrequests.store.ssl.enabled" : {
        "title" : "SSL/TLS Enabled",
        "type" : "object",
        "propertyOrder" : 0,
        "description" : "",
        "properties" : {
          "value" : {
            "type" : "boolean",
```

```
              "required" : false
            },
            "inherited" : {
              "type" : "boolean",
              "required" : true
            }
          }
        },
        "org.forgerock.services.uma.pendingrequests.store.starttls.enabled" : {
          "title" : "Start TLS",
          "type" : "object",
          "propertyOrder" : 1,
          "description" : "Specifies whether to use StartTLS for the connection.",
          "properties" : {
            "value" : {
              "type" : "boolean",
              "required" : false
            },
            "inherited" : {
              "type" : "boolean",
              "required" : true
            }
          }
        },
        "org.forgerock.services.uma.pendingrequests.store.directory.name" : {
          "title" : "Connection String(s)",
          "type" : "object",
          "propertyOrder" : 2,
          "description" : "An ordered list of connection strings for LDAP directories. Each connection
 string is composed as follows: <code>HOST:PORT[|SERVERID[|SITEID]]</code>, where server and site
 IDs are optional parameters that will prioritize that connection to use from the specified nodes.
 Multiple connection strings should be comma-separated, e.g. <code>host1:389,host2:50389|server1|
site1,host3:50389</code>.",
          "properties" : {
            "value" : {
              "type" : "string",
              "required" : false
            },
            "inherited" : {
              "type" : "boolean",
              "required" : true
            }
          }
        },
        "org.forgerock.services.uma.pendingrequests.store.loginid" : {
          "title" : "Login Id",
          "type" : "object",
          "propertyOrder" : 3,
          "description" : "",
          "properties" : {
            "value" : {
              "type" : "string",
              "required" : false
            },
            "inherited" : {
              "type" : "boolean",
              "required" : true
            }
          }
```

```
        },
        "org.forgerock.services.uma.pendingrequests.store.password" : {
          "title" : "Password",
          "type" : "object",
          "propertyOrder" : 4,
          "description" : "",
          "properties" : {
            "value" : {
              "type" : "string",
              "required" : false,
              "format" : "password"
            },
            "inherited" : {
              "type" : "boolean",
              "required" : true
            }
          }
        },
        "org.forgerock.services.uma.pendingrequests.store.heartbeat" : {
          "title" : "Heartbeat",
          "type" : "object",
          "propertyOrder" : 5,
          "description" : "",
          "properties" : {
            "value" : {
              "type" : "integer",
              "required" : false
            },
            "inherited" : {
              "type" : "boolean",
              "required" : true
            }
          }
        }
      }
    },
    "amconfig.org.forgerock.services.uma.labels.store.common.section" : {
      "title" : "UMA Resource Labels Store",
      "type" : "object",
      "propertyOrder" : 6,
      "properties" : {
        "org.forgerock.services.uma.labels.store.location" : {
          "title" : "Store Mode",
          "type" : "object",
          "propertyOrder" : 0,
          "description" : "",
          "properties" : {
            "value" : {
              "enum" : [ "default", "external" ],
              "options" : {
                "enum_titles" : [ "Default Token Store", "External Token Store" ]
              },
              "type" : "string",
              "required" : false
            },
            "inherited" : {
              "type" : "boolean",
              "required" : true
            }
```

```
        }
      },
      "org.forgerock.services.uma.labels.store.root.suffix" : {
        "title" : "Root Suffix",
        "type" : "object",
        "propertyOrder" : 1,
        "description" : "",
        "properties" : {
          "value" : {
            "type" : "string",
            "required" : false
          },
          "inherited" : {
            "type" : "boolean",
            "required" : true
          }
        }
      },
      "org.forgerock.services.uma.labels.store.max.connections" : {
        "title" : "Max Connections",
        "type" : "object",
        "propertyOrder" : 2,
        "description" : "",
        "properties" : {
          "value" : {
            "type" : "string",
            "required" : false
          },
          "inherited" : {
            "type" : "boolean",
            "required" : true
          }
        }
      }
    }
  },
  "amconfig.org.forgerock.services.uma.labels.store.external.section" : {
    "title" : "External UMA Resource Labels Store Configuration",
    "type" : "object",
    "propertyOrder" : 7,
    "properties" : {
      "org.forgerock.services.uma.labels.store.ssl.enabled" : {
        "title" : "SSL/TLS Enabled",
        "type" : "object",
        "propertyOrder" : 0,
        "description" : "",
        "properties" : {
          "value" : {
            "type" : "boolean",
            "required" : false
          },
          "inherited" : {
            "type" : "boolean",
            "required" : true
          }
        }
      },
      "org.forgerock.services.uma.labels.store.starttls.enabled" : {
        "title" : "Start TLS",
```

```
          "type" : "object",
          "propertyOrder" : 1,
          "description" : "Specifies whether to use StartTLS for the connection.",
          "properties" : {
            "value" : {
              "type" : "boolean",
              "required" : false
            },
            "inherited" : {
              "type" : "boolean",
              "required" : true
            }
          }
        },
        "org.forgerock.services.uma.labels.store.directory.name" : {
          "title" : "Connection String(s)",
          "type" : "object",
          "propertyOrder" : 2,
          "description" : "An ordered list of connection strings for LDAP directories. Each connection
 string is composed as follows: <code>HOST:PORT[|SERVERID[|SITEID]]</code>, where server and site
 IDs are optional parameters that will prioritize that connection to use from the specified nodes.
 Multiple connection strings should be comma-separated, e.g. <code>host1:389,host2:50389|server1|
site1,host3:50389</code>.",
          "properties" : {
            "value" : {
              "type" : "string",
              "required" : false
            },
            "inherited" : {
              "type" : "boolean",
              "required" : true
            }
          }
        },
        "org.forgerock.services.uma.labels.store.loginid" : {
          "title" : "Login Id",
          "type" : "object",
          "propertyOrder" : 3,
          "description" : "",
          "properties" : {
            "value" : {
              "type" : "string",
              "required" : false
            },
            "inherited" : {
              "type" : "boolean",
              "required" : true
            }
          }
        },
        "org.forgerock.services.uma.labels.store.password" : {
          "title" : "Password",
          "type" : "object",
          "propertyOrder" : 4,
          "description" : "",
          "properties" : {
            "value" : {
              "type" : "string",
              "required" : false,
```

```
              "format" : "password"
            },
            "inherited" : {
              "type" : "boolean",
              "required" : true
            }
          }
        },
        "org.forgerock.services.uma.labels.store.heartbeat" : {
          "title" : "Heartbeat",
          "type" : "object",
          "propertyOrder" : 5,
          "description" : "",
          "properties" : {
            "value" : {
              "type" : "integer",
              "required" : false
            },
            "inherited" : {
              "type" : "boolean",
              "required" : true
            }
          }
        }
      }
    }
  }
}
```

UmaPolicies

Realm Operations

Provides create, delete and query operations for UMA Policies

Resource path: `/users/{user}/uma/policies`

Resource version: `1.0`

create

Creates an UMA Policy

Usage:

```
am> create UmaPolicies --realm Realm --id id --body body --user user
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "$schema" : "http://json-schema.org/draft-04/schema#",
  "description" : "A policy defining who can access a particular resource set",
  "type" : "object",
  "title" : "UMA Policy",
  "properties" : {
    "policyId" : {
      "type" : "string",
      "title" : "Policy ID",
      "description" : "The ID must correspond with an existing resource set ID"
    },
    "permissions" : {
      "type" : "array",
      "title" : "Permissions",
      "description" : "A list of subjects and the scopes they are allowed access to",
      "items" : {
        "type" : "object",
        "properties" : {
          "subject" : {
            "type" : "string",
            "title" : "Subject",
            "description" : "The username of the subject"
          },
          "scopes" : {
            "type" : "array",
            "title" : "Scopes",
            "description" : "The scopes that the user is allowed access to",
            "items" : {
              "type" : "string"
            }
          }
        }
      }
    }
  }
}
```

--user

Provides create, delete and query operations for UMA Policies

delete

Deletes an UMA Policy

Usage:

```
am> delete UmaPolicies --realm Realm --id id --user user
```

Parameters:

--id

The unique identifier for the resource.

--user

Provides create, delete and query operations for UMA Policies

query

Queries an UMA Policy

Usage:

```
am> query UmaPolicies --realm Realm --filter filter --user user
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all. Fields that can be queried: [*]

--user

Provides create, delete and query operations for UMA Policies

read

Reads an UMA Policy

Usage:

```
am> read UmaPolicies --realm Realm --id id --user user
```

Parameters:

--id

The unique identifier for the resource.

--user

Provides create, delete and query operations for UMA Policies

update

Updates an UMA Policy

Usage:

```
am> update UmaPolicies --realm Realm --id id --body body --user user
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "$schema" : "http://json-schema.org/draft-04/schema#",
  "description" : "A policy defining who can access a particular resource set",
  "type" : "object",
  "title" : "UMA Policy",
  "properties" : {
    "policyId" : {
      "type" : "string",
      "title" : "Policy ID",
      "description" : "The ID must correspond with an existing resource set ID"
    },
    "permissions" : {
      "type" : "array",
      "title" : "Permissions",
      "description" : "A list of subjects and the scopes they are allowed access to",
      "items" : {
        "type" : "object",
        "properties" : {
          "subject" : {
            "type" : "string",
            "title" : "Subject",
            "description" : "The username of the subject"
          },
          "scopes" : {
            "type" : "array",
            "title" : "Scopes",
            "description" : "The scopes that the user is allowed access to",
            "items" : {
              "type" : "string"
            }
          }
        }
      }
    }
  }
}
```

--user

Provides create, delete and query operations for UMA Policies

UmaProvider

Realm Operations

Resource path: `/realm-config/services/uma`

Resource version: `1.0`

create

Usage:

```
am> create UmaProvider --realm Realm --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "resharingMode" : {
      "title" : "Re-Sharing Mode",
      "description" : "Specifies whether re-sharing is off or on implicitly for all users, allowing
 all users to re-share resources that have been shared with them.",
      "propertyOrder" : 800,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "userProfileLocaleAttribute" : {
      "title" : "User profile preferred Locale attribute",
      "description" : "User profile attribute storing the user's preferred locale.",
      "propertyOrder" : 700,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "grantRptConditions" : {
      "title" : "Grant RPTs...",
      "description" : "In UMA, scope comes from both the permission ticket and from the token request.
 An RPT is always granted when all scope matches, and is never granted when no scope matches. You can
 configure when RPTs are granted for partial match conditions here. For more information, see the UMA
 Grant Type specification section onAuthorization Assessment and Results Determination.",
      "propertyOrder" : 900,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "deletePoliciesOnDeleteRS" : {
      "title" : "Delete user policies when Resource Server is removed",
      "description" : "Delete all user policies that relate to a Resource Server when removing the
 OAuth2 agent entry or removing the <code>uma_protection</code> scope from the OAuth2 agent.",
      "propertyOrder" : 300,
```

```
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "permissionTicketLifetime" : {
      "title" : "Permission Ticket Lifetime (seconds)",
      "description" : "The maximum life of a permission ticket before it expires, in seconds.",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "emailResourceOwnerOnPendingRequestCreation" : {
      "title" : "Email Resource Owner on Pending Request creation",
      "description" : "Specifies whether to send an email to the Resource Owner when a Pending Request
 is created when a Requesting Party requests authorization to a resource.",
      "propertyOrder" : 500,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "deleteResourceSetsOnDeleteRS" : {
      "title" : "Delete resources when Resource Server is removed",
      "description" : "Delete all resources that relate to a Resource Server when removing the OAuth2
 agent entry or removing the <code>uma_protection</code> scope from the OAuth2 agent.",
      "propertyOrder" : 400,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "emailRequestingPartyOnPendingRequestApproval" : {
      "title" : "Email Requesting Party on Pending Request approval",
      "description" : "Specifies whether to send an email to the Requesting Party when a Pending
 Request is approved by the Resource Owner.",
      "propertyOrder" : 600,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "pendingRequestsEnabled" : {
      "title" : "Pending Requests Enabled",
      "description" : "Specifies whether to use the Pending Requests subsystem that notifies the
 resource owner that an attempt to access a resource was made.",
      "propertyOrder" : 450,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    }
  }
}
```

delete

Usage:

```
am> delete UmaProvider --realm Realm
```

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action UmaProvider --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action UmaProvider --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action UmaProvider --realm Realm --actionName nextdescendents
```

read

Usage:

```
am> read UmaProvider --realm Realm
```

update

Usage:

```
am> update UmaProvider --realm Realm --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "resharingMode" : {
      "title" : "Re-Sharing Mode",
      "description" : "Specifies whether re-sharing is off or on implicitly for all users, allowing
 all users to re-share resources that have been shared with them.",
      "propertyOrder" : 800,
      "required" : true,
      "type" : "string",
```

```
      "exampleValue" : ""
    },
    "userProfileLocaleAttribute" : {
      "title" : "User profile preferred Locale attribute",
      "description" : "User profile attribute storing the user's preferred locale.",
      "propertyOrder" : 700,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "grantRptConditions" : {
      "title" : "Grant RPTs...",
      "description" : "In UMA, scope comes from both the permission ticket and from the token request.
An RPT is always granted when all scope matches, and is never granted when no scope matches. You can
configure when RPTs are granted for partial match conditions here. For more information, see the UMA
Grant Type specification section onAuthorization Assessment and Results Determination.",
      "propertyOrder" : 900,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "deletePoliciesOnDeleteRS" : {
      "title" : "Delete user policies when Resource Server is removed",
      "description" : "Delete all user policies that relate to a Resource Server when removing the
OAuth2 agent entry or removing the <code>uma_protection</code> scope from the OAuth2 agent.",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "permissionTicketLifetime" : {
      "title" : "Permission Ticket Lifetime (seconds)",
      "description" : "The maximum life of a permission ticket before it expires, in seconds.",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "emailResourceOwnerOnPendingRequestCreation" : {
      "title" : "Email Resource Owner on Pending Request creation",
      "description" : "Specifies whether to send an email to the Resource Owner when a Pending Request
is created when a Requesting Party requests authorization to a resource.",
      "propertyOrder" : 500,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "deleteResourceSetsOnDeleteRS" : {
      "title" : "Delete resources when Resource Server is removed",
      "description" : "Delete all resources that relate to a Resource Server when removing the OAuth2
agent entry or removing the <code>uma_protection</code> scope from the OAuth2 agent.",
      "propertyOrder" : 400,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
```

```
    "emailRequestingPartyOnPendingRequestApproval" : {
      "title" : "Email Requesting Party on Pending Request approval",
      "description" : "Specifies whether to send an email to the Requesting Party when a Pending
 Request is approved by the Resource Owner.",
      "propertyOrder" : 600,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "pendingRequestsEnabled" : {
      "title" : "Pending Requests Enabled",
      "description" : "Specifies whether to use the Pending Requests subsystem that notifies the
 resource owner that an attempt to access a resource was made.",
      "propertyOrder" : 450,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    }
  }
}
```

Global Operations

Resource path: `/global-config/services/uma`

Resource version: `1.0`

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action UmaProvider --global --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action UmaProvider --global --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action UmaProvider --global --actionName nextdescendents
```

read

Usage:

```
am> read UmaProvider --global
```

update

Usage:

```
am> update UmaProvider --global --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "defaults" : {
      "properties" : {
        "deletePoliciesOnDeleteRS" : {
          "title" : "Delete user policies when Resource Server is removed",
          "description" : "Delete all user policies that relate to a Resource Server when removing the
 OAuth2 agent entry or removing the <code>uma_protection</code> scope from the OAuth2 agent.",
          "propertyOrder" : 300,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "grantRptConditions" : {
          "title" : "Grant RPTs...",
          "description" : "In UMA, scope comes from both the permission ticket and from the token
 request. An RPT is always granted when all scope matches, and is never granted when no scope matches.
 You can configure when RPTs are granted for partial match conditions here. For more information, see
 the UMA Grant Type specification section onAuthorization Assessment and Results Determination.",
          "propertyOrder" : 900,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "emailResourceOwnerOnPendingRequestCreation" : {
          "title" : "Email Resource Owner on Pending Request creation",
          "description" : "Specifies whether to send an email to the Resource Owner when a Pending
 Request is created when a Requesting Party requests authorization to a resource.",
          "propertyOrder" : 500,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "pendingRequestsEnabled" : {
```

```
          "title" : "Pending Requests Enabled",
          "description" : "Specifies whether to use the Pending Requests subsystem that notifies the
 resource owner that an attempt to access a resource was made.",
          "propertyOrder" : 450,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "deleteResourceSetsOnDeleteRS" : {
          "title" : "Delete resources when Resource Server is removed",
          "description" : "Delete all resources that relate to a Resource Server when removing the
 OAuth2 agent entry or removing the <code>uma_protection</code> scope from the OAuth2 agent.",
          "propertyOrder" : 400,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "permissionTicketLifetime" : {
          "title" : "Permission Ticket Lifetime (seconds)",
          "description" : "The maximum life of a permission ticket before it expires, in seconds.",
          "propertyOrder" : 200,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "emailRequestingPartyOnPendingRequestApproval" : {
          "title" : "Email Requesting Party on Pending Request approval",
          "description" : "Specifies whether to send an email to the Requesting Party when a Pending
 Request is approved by the Resource Owner.",
          "propertyOrder" : 600,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "userProfileLocaleAttribute" : {
          "title" : "User profile preferred Locale attribute",
          "description" : "User profile attribute storing the user's preferred locale.",
          "propertyOrder" : 700,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "resharingMode" : {
          "title" : "Re-Sharing Mode",
          "description" : "Specifies whether re-sharing is off or on implicitly for all users,
 allowing all users to re-share resources that have been shared with them.",
          "propertyOrder" : 800,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      },
      "type" : "object",
      "title" : "Realm Defaults"
    }
  }
}
```

UmaResourceSetLabels

Realm Operations

Provides create, delete and query operations for UMA resource set labels

Resource path: `/users/{user}/oauth2/resources/labels`

Resource version: `1.0`

create

Creates a UMA Resource Set Label

Usage:

```
am> create UmaResourceSetLabels --realm Realm --id id --body body --user user
```

Parameters:

`--id`

The unique identifier for the resource.

`--body`

The resource in JSON format, described by the following JSON schema:

```
{
  "description" : "Represents a UMA Resource Set Label",
  "id" : "urn:jsonschema:org:forgerock:openam:oauth2:resources:labels:ResourceSetLabel",
  "type" : "object",
  "title" : "UMA Resource Set Label",
  "properties" : {
    "id" : {
      "type" : "string",
      "description" : "The unique identifier of the resource set label",
      "title" : "Id"
    },
    "name" : {
      "type" : "string",
      "description" : "The displayed text of the label",
      "title" : "Name"
    },
    "type" : {
      "type" : "string",
      "description" : "The type of the label e.g. 'System'",
      "title" : "Type",
      "enum" : [ "STAR", "USER", "SYSTEM" ]
    },
    "resourceSetIds" : {
      "type" : "array",
      "items" : {
        "type" : "string"
      }
    }
  }
}
```

--user

Provides create, delete and query operations for UMA resource set labels

delete

Deletes a UMA Resource Set Label

Usage:

```
am> delete UmaResourceSetLabels --realm Realm --id id --user user
```

Parameters:

--id

The unique identifier for the resource.

--user

Provides create, delete and query operations for UMA resource set labels

query

Queries the collection of UMA labels

Usage:

```
am> query UmaResourceSetLabels --realm Realm --filter filter --user user
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all. Fields that can be queried: [*]

--user

Provides create, delete and query operations for UMA resource set labels

UmaUserAuditHistory

Realm Operations

Provides access to UMA auditing history for a user

Resource path: `/users/{user}/uma/auditHistory`

Resource version: `1.0`

getHistory

Returns the audit history of a user

Usage:

```
am> action UmaUserAuditHistory --realm Realm --user user --actionName getHistory
```

Parameters:

--user

Provides access to UMA auditing history for a user

query

Queries the collection of auditing history

Usage:

```
am> query UmaUserAuditHistory --realm Realm --filter filter --user user
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all. Fields that can be queried: [*]

--user

Provides access to UMA auditing history for a user

User

Realm Operations

Resource path: `/realm-config/services/user`

Resource version: `1.0`

create

Usage:

```
am> create User --realm Realm --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "dynamic" : {
      "properties" : {
        "adminDNStartingView" : {
          "title" : "Administrator DN Starting View",
          "description" : "Specifies the DN for the initial screen when the OpenAM administrator
 successfully logs in to the OpenAM console.",
          "propertyOrder" : 200,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "defaultUserStatus" : {
          "title" : "Default User Status",
          "description" : "Inactive users cannot authenticate, though OpenAM stores their profiles.",
          "propertyOrder" : 300,
          "required" : true,
          "type" : "string",
```

```
          "exampleValue" : ""
        },
        "preferredTimezone" : {
          "title" : "User Preferred Timezone",
          "description" : "Time zone for accessing OpenAM console.",
          "propertyOrder" : 100,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      },
      "type" : "object",
      "title" : "Dynamic Attributes"
    }
  }
}
```

delete

Usage:

```
am> delete User --realm Realm
```

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action User --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action User --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action User --realm Realm --actionName nextdescendents
```

read

Usage:

```
am> read User --realm Realm
```

update

Usage:

```
am> update User --realm Realm --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "dynamic" : {
      "properties" : {
        "adminDNStartingView" : {
          "title" : "Administrator DN Starting View",
          "description" : "Specifies the DN for the initial screen when the OpenAM administrator
 successfully logs in to the OpenAM console.",
          "propertyOrder" : 200,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "defaultUserStatus" : {
          "title" : "Default User Status",
          "description" : "Inactive users cannot authenticate, though OpenAM stores their profiles.",
          "propertyOrder" : 300,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "preferredTimezone" : {
          "title" : "User Preferred Timezone",
          "description" : "Time zone for accessing OpenAM console.",
          "propertyOrder" : 100,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      },
      "type" : "object",
      "title" : "Dynamic Attributes"
    }
  }
}
```

Global Operations

Resource path: `/global-config/services/user`

Resource version: `1.0`

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action User --global --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action User --global --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action User --global --actionName nextdescendents
```

read

Usage:

```
am> read User --global
```

update

Usage:

```
am> update User --global --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
```

```
    "dynamic" : {
      "properties" : {
        "adminDNStartingView" : {
          "title" : "Administrator DN Starting View",
          "description" : "Specifies the DN for the initial screen when the OpenAM administrator
 successfully logs in to the OpenAM console.",
          "propertyOrder" : 200,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "defaultUserStatus" : {
          "title" : "Default User Status",
          "description" : "Inactive users cannot authenticate, though OpenAM stores their profiles.",
          "propertyOrder" : 300,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "preferredTimezone" : {
          "title" : "User Preferred Timezone",
          "description" : "Time zone for accessing OpenAM console.",
          "propertyOrder" : 100,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      },
      "type" : "object",
      "title" : "Dynamic Attributes"
    }
  }
}
```

UserGroups

Realm Operations

The User Groups resource allows an admin to query which groups a particular user belongs to. The only supported method is query

Resource path: `/users/{user}/groups`

Resource version: `1.0`

query

Query the user's groups

Usage:

```
am> query UserGroups --realm Realm --filter filter --user user
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all. Fields that can be queried: [*]

--user

The User Groups resource allows an admin to query which groups a particular user belongs to. The only supported method is query

updateMemberships

Usage:

```
am> action UserGroups --realm Realm --body body --user user --actionName updateMemberships
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "$schema" : "http://json-schema.org/draft-04/schema#",
  "description" : "",
  "title" : "User groups schema",
  "type" : "object",
  "properties" : {
    "groups" : {
      "type" : "array",
      "title" : "Name",
      "description" : "The name of the group",
      "items" : {
        "type" : "string"
      }
    }
  }
}
```

--user

The User Groups resource allows an admin to query which groups a particular user belongs to. The only supported method is query

UserPolicies

Realm Operations

The User Policy resource endpoint is responsible for managing a user's policies. The available operations are create, read, update, delete, query. Policies are realm specific, hence the URI for the

policies API can contain a realm component. If the realm is not specified in the URI, the top level realm is used.

Resource path: `/users/{user}/policies`

Resource version: `1.0`

create

Create new policy

Usage:

```
am> create UserPolicies --realm Realm --id id --body body --user user
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "$schema" : "http://json-schema.org/draft-04/schema#",
  "description" : "Json schema for the policy resource",
  "title" : "Policy Resource Schema",
  "type" : "object",
  "properties" : {
    "name" : {
      "title" : "Name",
      "description" : "String matching the name of the application",
      "type" : "string"
    },
    "active" : {
      "title" : "Active flag",
      "description" : "Boolean indicating whether OpenAM considers the policy active for evaluation
 purposes, defaults to false",
      "type" : "boolean"
    },
    "description" : {
      "title" : "Description",
      "description" : "String describing the policy",
      "type" : "string"
    },
    "applicationName" : {
      "title" : "Application name",
      "description" : "String containing the application name, such as \"iPlanetAMWebAgentService\",
 or \"mypolicyset\"",
      "type" : "string"
    },
    "actionValues" : {
      "title" : "Action values",
```

```
     "description" : "Set of string action names, each set to a boolean indicating whether the action
is allowed. Chosen from the available actions provided by the associated Managing Resource Types
resource type",
     "type" : "object",
     "additionalProperties" : {
       "type" : "boolean"
     }
   },
   "resources" : {
     "title" : "Resources",
     "description" : "List of the resource name pattern strings to which the policy applies. Must
conform to the pattern templates provided by the associated Managing Resource Types resource type",
     "type" : "array",
     "items" : {
       "type" : "string"
     }
   },
   "subject" : {
     "title" : "Subject",
     "description" : "Specifies the subject conditions to which the policy applies, where subjects
can be combined by using the built-in types \"AND\", \"OR\", and \"NOT\", and where subject
implementations are pluggable",
     "type" : "object"
   },
   "condition" : {
     "title" : "Condition",
     "description" : "Specifies environment conditions, where conditions can be combined by using the
built-in types \"AND\", \"OR\", and \"NOT\", and where condition implementations are pluggable",
     "type" : "object",
     "properties" : {
       "type" : {
         "type" : "string"
       },
       "conditions" : {
         "type" : "array",
         "title" : "Condition",
         "description" : "Specifies environment conditions, where conditions can be combined by using
the built-in types \"AND\", \"OR\", and \"NOT\", and where condition implementations are pluggable",
         "items" : {
           "type" : "object"
         }
       }
     }
   },
   "resourceTypeUuid" : {
     "title" : "Resource Type UUID",
     "description" : "The UUIDs of the resource type associated with the policy",
     "type" : "string"
   },
   "resourceAttributes" : {
     "title" : "Resource Attributes",
     "description" : "List of attributes to return with decisions. These attributes are known as
response attributes",
     "type" : "array",
     "items" : {
       "type" : "object"
     }
   },
   "lastModifiedBy" : {
```

```
      "title" : "Last Modified By",
      "description" : "A string containing the universal identifier DN of the subject that most
 recently updated the policy",
      "type" : "string"
    },
    "lastModifiedDate" : {
      "title" : "Last Modified date",
      "description" : "An integer containing the last modified date and time, in number of seconds",
      "type" : "string"
    },
    "createdBy" : {
      "title" : "Created By",
      "description" : "A string containing the universal identifier DN of the subject that created the
 policy",
      "type" : "string"
    },
    "creationDate" : {
      "title" : "Creation Date",
      "description" : "An integer containing the creation date and time, in number of seconds",
      "type" : "string"
    }
  }
}
```

--user

The User Policy resource endpoint is responsible for managing a user's policies. The available operations are create, read, update, delete, query. Policies are realm specific, hence the URI for the policies API can contain a realm component. If the realm is not specified in the URI, the top level realm is used.

delete

Delete policy

Usage:

```
am> delete UserPolicies --realm Realm --id id --user user
```

Parameters:

--id

The unique identifier for the resource.

--user

The User Policy resource endpoint is responsible for managing a user's policies. The available operations are create, read, update, delete, query. Policies are realm specific, hence the URI for the policies API can contain a realm component. If the realm is not specified in the URI, the top level realm is used.

query

Query the stored policies

Usage:

```
am> query UserPolicies --realm Realm --filter filter --user user
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all. Fields that can be queried: [*]

--user

The User Policy resource endpoint is responsible for managing a user's policies. The available operations are create, read, update, delete, query. Policies are realm specific, hence the URI for the policies API can contain a realm component. If the realm is not specified in the URI, the top level realm is used.

read

Read policy

Usage:

```
am> read UserPolicies --realm Realm --id id --user user
```

Parameters:

--id

The unique identifier for the resource.

--user

The User Policy resource endpoint is responsible for managing a user's policies. The available operations are create, read, update, delete, query. Policies are realm specific, hence the URI for the policies API can contain a realm component. If the realm is not specified in the URI, the top level realm is used.

update

Update an existing policy

Usage:

```
am> update UserPolicies --realm Realm --id id --body body --user user
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "$schema" : "http://json-schema.org/draft-04/schema#",
  "description" : "Json schema for the policy resource",
  "title" : "Policy Resource Schema",
  "type" : "object",
  "properties" : {
    "name" : {
      "title" : "Name",
      "description" : "String matching the name of the application",
      "type" : "string"
    },
    "active" : {
      "title" : "Active flag",
      "description" : "Boolean indicating whether OpenAM considers the policy active for evaluation
 purposes, defaults to false",
      "type" : "boolean"
    },
    "description" : {
      "title" : "Description",
      "description" : "String describing the policy",
      "type" : "string"
    },
    "applicationName" : {
      "title" : "Application name",
      "description" : "String containing the application name, such as \"iPlanetAMWebAgentService\",
 or \"mypolicyset\"",
      "type" : "string"
    },
    "actionValues" : {
      "title" : "Action values",
      "description" : "Set of string action names, each set to a boolean indicating whether the action
 is allowed. Chosen from the available actions provided by the associated Managing Resource Types
 resource type",
      "type" : "object",
      "additionalProperties" : {
        "type" : "boolean"
      }
    },
    "resources" : {
      "title" : "Resources",
      "description" : "List of the resource name pattern strings to which the policy applies. Must
 conform to the pattern templates provided by the associated Managing Resource Types resource type",
      "type" : "array",
      "items" : {
        "type" : "string"
      }
    },
    "subject" : {
      "title" : "Subject",
```

```
     "description" : "Specifies the subject conditions to which the policy applies, where subjects
can be combined by using the built-in types \"AND\", \"OR\", and \"NOT\", and where subject
implementations are pluggable",
     "type" : "object"
   },
   "condition" : {
     "title" : "Condition",
     "description" : "Specifies environment conditions, where conditions can be combined by using the
built-in types \"AND\", \"OR\", and \"NOT\", and where condition implementations are pluggable",
     "type" : "object",
     "properties" : {
       "type" : {
         "type" : "string"
       },
       "conditions" : {
         "type" : "array",
         "title" : "Condition",
         "description" : "Specifies environment conditions, where conditions can be combined by using
the built-in types \"AND\", \"OR\", and \"NOT\", and where condition implementations are pluggable",
         "items" : {
           "type" : "object"
         }
       }
     }
   },
   "resourceTypeUuid" : {
     "title" : "Resource Type UUID",
     "description" : "The UUIDs of the resource type associated with the policy",
     "type" : "string"
   },
   "resourceAttributes" : {
     "title" : "Resource Attributes",
     "description" : "List of attributes to return with decisions. These attributes are known as
response attributes",
     "type" : "array",
     "items" : {
       "type" : "object"
     }
   },
   "lastModifiedBy" : {
     "title" : "Last Modified By",
     "description" : "A string containing the universal identifier DN of the subject that most
recently updated the policy",
     "type" : "string"
   },
   "lastModifiedDate" : {
     "title" : "Last Modified date",
     "description" : "An integer containing the last modified date and time, in number of seconds",
     "type" : "string"
   },
   "createdBy" : {
     "title" : "Created By",
     "description" : "A string containing the universal identifier DN of the subject that created the
policy",
     "type" : "string"
   },
   "creationDate" : {
     "title" : "Creation Date",
     "description" : "An integer containing the creation date and time, in number of seconds",
```

```
      "type" : "string"
    }
  }
}
```

--user

The User Policy resource endpoint is responsible for managing a user's policies. The available operations are create, read, update, delete, query. Policies are realm specific, hence the URI for the policies API can contain a realm component. If the realm is not specified in the URI, the top level realm is used.

UserRegistration

Realm Operations

Self Service endpoint for registering a new user

Resource path: `/selfservice/userRegistration`

Resource version: `1.0`

read

Initialise the user registration process.A set of requirements will be returned that will need to be fulfilled and sent to the submitRequirements action.

Usage:

```
am> read UserRegistration --realm Realm
```

submitRequirements

Submit some fulfilled requirements. Returns either a completion status, or a token along with some more requirements. If requirements are returned, they should be submitted with the token as a fresh request to this action.

Usage:

```
am> action UserRegistration --realm Realm --body body --actionName submitRequirements
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "$schema" : "http://json-schema.org/draft-04/schema#",
  "description" : "The structure of a request to the submitRequirements action.",
  "type" : "object",
  "title" : "Submit requirements structure",
  "properties" : {
    "token" : {
      "type" : "string",
      "title" : "Token",
      "description" : "The token returned from the previous submitRequirements request."
    },
    "input" : {
      "type" : "object",
      "title" : "Input",
      "description" : "The input as collected from the new user. This object must conform to the JSON
 Schema of the requirements property from the last response.",
      "patternProperties" : {
        ".*" : {
          "type" : "any",
          "title" : "Input Property",
          "description" : "Valid content according to the received JSON Schema."
        }
      }
    }
  },
  "required" : [ "input" ]
}
```

UserSelfService

Realm Operations

Resource path: `/realm-config/services/selfService`

Resource version: `1.0`

create

Usage:

```
am> create UserSelfService --realm Realm --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
```

```
    "userRegistration" : {
      "type" : "object",
      "title" : "User Registration",
      "propertyOrder" : 1,
      "properties" : {
        "userRegisteredDestination" : {
          "title" : "Destination After Successful Self-Registration",
          "description" : "Specifies the action to be taken after a user successfully registers
 a new account. Choose from:<ul><li><code>default</code>. User is sent to a success page without
 being logged in.</li><li><code>login</code>. User is sent to the login page to authenticate.</
li><li><code>autologin</code>. User is automatically logged in and sent to the appropriate page.</
li></ul>",
          "propertyOrder" : 161,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "userRegistrationEnabled" : {
          "title" : "User Registration",
          "description" : "If enabled, new users can sign up for an account.",
          "propertyOrder" : 90,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "userRegistrationEmailVerificationEnabled" : {
          "title" : "Email Verification",
          "description" : "If enabled, users who self-register must perform email address
 verification.",
          "propertyOrder" : 110,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "userRegistrationCaptchaEnabled" : {
          "title" : "Captcha",
          "description" : "If enabled, users must pass a Google reCAPTCHA challenge during user self-
registration to mitigate against software bots.",
          "propertyOrder" : 100,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "userRegistrationEmailBody" : {
          "title" : "Outgoing Email Body",
          "description" : "Customize the User Self-Registration verification email body text. Format
 is: <code>locale|body text</code>.",
          "propertyOrder" : 150,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "userRegistrationEmailSubject" : {
          "title" : "Outgoing Email Subject",
          "description" : "Customize the User Self-Registration verification email subject text.
 Format is <code>locale|subject text</code>.",
```

```
          "propertyOrder" : 140,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "userRegistrationKbaEnabled" : {
          "title" : "Security Questions",
          "description" : "If enabled, users must set up their security questions during the self-
registration process.",
          "propertyOrder" : 120,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "userRegistrationValidUserAttributes" : {
          "title" : "Valid Creation Attributes",
          "description" : "Specifies a whitelist of user attributes that can be set during user
 creation.",
          "propertyOrder" : 160,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "userRegistrationEmailVerificationFirstEnabled" : {
          "title" : "Verify Email before User Detail",
          "description" : "If enabled, email address verification will be performed first before user
 details screen is displayed. This will take effect only if Verify Email is enabled.",
          "propertyOrder" : 110,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "userRegistrationTokenTTL" : {
          "title" : "Token Lifetime (seconds)",
          "description" : "Maximum lifetime of the token allowing User Self-Registration, in
 seconds.",
          "propertyOrder" : 130,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        }
      }
    },
    "generalConfig" : {
      "type" : "object",
      "title" : "General Configuration",
      "propertyOrder" : 0,
      "properties" : {
        "validQueryAttributes" : {
          "title" : "Valid Query Attributes",
          "description" : "Specifies the valid query attributes used to search for the user. This is a
 list of attributes used to identify your account for forgotten password and forgotten username.",
          "propertyOrder" : 80,
```

```
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "captchaVerificationUrl" : {
          "title" : "Google Re-captcha Verification URL",
          "description" : "Google reCAPTCHA plugin verification URL.",
          "propertyOrder" : 40,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "captchaSecretKey" : {
          "title" : "Google reCAPTCHA Secret Key",
          "description" : "Google reCAPTCHA plugin secret key.",
          "propertyOrder" : 30,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "kbaQuestions" : {
          "title" : "Security Questions",
          "description" : "Specifies the default set of knowledge-based authentication (KBA) security
 questions. The security questions can be set for the User Self-Registration, forgotten password
 reset, and forgotten username services, respectively.<p><p>Format is <code>unique key|locale|
question</code>.",
          "propertyOrder" : 50,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "captchaSiteKey" : {
          "title" : "Google reCAPTCHA Site Key",
          "description" : "Google reCAPTCHA plugin site key.",
          "propertyOrder" : 20,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "signingSecretKeyAlias" : {
          "title" : "Signing Secret Key Alias",
          "description" : "A signing secret key alias in the OpenAM server's JCEKS keystore. Used to
 sign the JWT token that OpenAM uses to track end users during User Self-Service operations.",
          "propertyOrder" : 10,
          "required" : true,
          "type" : "string",
          "exampleValue" : "selfservicesigntest"
        },
        "encryptionKeyPairAlias" : {
          "title" : "Encryption Key Pair Alias",
          "description" : "An encryption key alias in the OpenAM server's JCEKS keystore. Used to
 encrypt the JWT token that OpenAM uses to track end users during User Self-Service operations.",
          "propertyOrder" : 0,
```

```
          "required" : true,
          "type" : "string",
          "exampleValue" : "selfserviceenctest"
        },
        "minimumAnswersToDefine" : {
          "title" : "Minimum Answers to Define",
          "description" : "Specifies the minimum number of KBA answers that users must define.",
          "propertyOrder" : 60,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "minimumAnswersToVerify" : {
          "title" : "Minimum Answers to Verify",
          "description" : "Specifies the minimum number of KBA questions that users need to answer
 to be granted the privilege to carry out an action, such as registering for an account, resetting a
 password, or retrieving a username. Specify a value from <code>0</code> to <code>50</code>.",
          "propertyOrder" : 70,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        }
      }
    },
    "advancedConfig" : {
      "type" : "object",
      "title" : "Advanced Configuration",
      "propertyOrder" : 5,
      "properties" : {
        "userRegistrationServiceConfigClass" : {
          "title" : "User Registration Service Config Provider Class",
          "description" : "Specifies the provider class to configure any custom plugins.",
          "propertyOrder" : 350,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "userRegistrationConfirmationUrl" : {
          "title" : "User Registration Confirmation Email URL",
          "description" : "Specifies the confirmation URL that the user receives during the self-
registration process. The <code>${realm}</code> string is replaced with the current realm.",
          "propertyOrder" : 330,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "forgottenPasswordConfirmationUrl" : {
          "title" : "Forgotten Password Confirmation Email URL",
          "description" : "Specifies the confirmation URL that the user receives after confirming
 their identity during the forgotten password process. The <code>${realm}</code> string is replaced
 with the current realm.",
          "propertyOrder" : 340,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "forgottenUsernameServiceConfigClass" : {
          "title" : "Forgotten Username Service Config Provider Class",
          "description" : "Specifies the provider class to configure any custom plugins.",
```

```
          "propertyOrder" : 370,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "forgottenPasswordServiceConfigClass" : {
          "title" : "Forgotten Password Service Config Provider Class",
          "description" : "Specifies the provider class to configure any custom plugins.",
          "propertyOrder" : 360,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "forgottenUsername" : {
      "type" : "object",
      "title" : "Forgotten Username",
      "propertyOrder" : 3,
      "properties" : {
        "forgottenUsernameEnabled" : {
          "title" : "Forgotten Username",
          "description" : "If enabled, users can retrieve their forgotten username.",
          "propertyOrder" : 240,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "forgottenUsernameKbaEnabled" : {
          "title" : "Security Questions",
          "description" : "If enabled, users must answer their security questions during the forgotten
username process.",
          "propertyOrder" : 260,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "forgottenUsernameEmailSubject" : {
          "title" : "Outgoing Email Subject",
          "description" : "Customizes the forgotten username email subject text. Format is
<code>locale|subject text</code>.",
          "propertyOrder" : 300,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "forgottenUsernameCaptchaEnabled" : {
          "title" : "Captcha",
          "description" : "If enabled, users must pass a Google reCAPTCHA challenge during the
forgotten username retrieval process to mitigate against software bots.",
          "propertyOrder" : 250,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "forgottenUsernameEmailBody" : {
```

```
          "title" : "Outgoing Email Body",
          "description" : "Customizes the forgotten username email body text. Format is <code>locale|
body text</code>.",
          "propertyOrder" : 310,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "forgottenUsernameShowUsernameEnabled" : {
          "title" : "Show Username",
          "description" : "If enabled, users see their forgotten username on the browser page.",
          "propertyOrder" : 280,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "forgottenUsernameTokenTTL" : {
          "title" : "Token LifeTime (seconds)",
          "description" : "Maximum lifetime for the token allowing forgotten username, in seconds.",
          "propertyOrder" : 290,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "forgottenUsernameEmailUsernameEnabled" : {
          "title" : "Email Username",
          "description" : "If enabled, users receive their forgotten username by email.",
          "propertyOrder" : 270,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        }
      }
    },
    "forgottenPassword" : {
      "type" : "object",
      "title" : "Forgotten Password",
      "propertyOrder" : 2,
      "properties" : {
        "forgottenPasswordTokenTTL" : {
          "title" : "Token Lifetime (seconds)",
          "description" : "Maximum lifetime for the token allowing forgotten password reset, in
 seconds.<p><p>Specify a value from <code>0</code> to <code>2147483647</code>.",
          "propertyOrder" : 210,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "forgottenPasswordKbaEnabled" : {
          "title" : "Security Questions",
          "description" : "If enabled, users must answer their security questions during the forgotten
 password process.",
          "propertyOrder" : 200,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
```

```
        },
        "forgottenPasswordEnabled" : {
          "title" : "Forgotten Password",
          "description" : "If enabled, users can reset their forgotten password.",
          "propertyOrder" : 170,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "forgottenPasswordEmailVerificationEnabled" : {
          "title" : "Email Verification",
          "description" : "If enabled, users who reset passwords must perform email address
 verification.",
          "propertyOrder" : 190,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "forgottenPasswordCaptchaEnabled" : {
          "title" : "Captcha",
          "description" : "If enabled, users must pass a Google reCAPTCHA challenge during password
 reset to mitigate against software bots.",
          "propertyOrder" : 180,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "numberOfAllowedAttempts" : {
          "title" : "Lock Out After number of attempts",
          "description" : "Can be set to 1 or more attempts for a user to correctly answer all their
 security questions. After the number of configured attempts the user has not correctly answered them
 the password reset feature will be disabled.",
          "propertyOrder" : 202,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "forgottenPasswordEmailBody" : {
          "title" : "Outgoing Email Body",
          "description" : "Customize the forgotten password email body text. Format is <code>locale|
body text</code>.",
          "propertyOrder" : 230,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "numberOfAttemptsEnforced" : {
          "title" : "Enforce password reset lockout",
          "description" : "If enabled, users will be prevented from resetting their password after the
 configured number of failed attempts.",
          "propertyOrder" : 201,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "forgottenPasswordEmailSubject" : {
```

```
          "title" : "Outgoing Email Subject",
          "description" : "Customize the forgotten password email subject text. Format is
 <code>locale|subject text</code>.",
          "propertyOrder" : 220,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        }
      }
    },
    "profileManagement" : {
      "type" : "object",
      "title" : "Profile Management",
      "propertyOrder" : 4,
      "properties" : {
        "profileAttributeWhitelist" : {
          "title" : "Self readable attributes",
          "description" : "Specifies the list of attributes that users can view when accessing their
 user profile.",
          "propertyOrder" : 325,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "profileProtectedUserAttributes" : {
          "title" : "Protected Update Attributes",
          "description" : "Specifies a profile's protected user attributes, which causes re-
authentication when the user attempts to modify these attributes.",
          "propertyOrder" : 320,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        }
      }
    }
  }
}
```

delete

Usage:

```
am> delete UserSelfService --realm Realm
```

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action UserSelfService --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action UserSelfService --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action UserSelfService --realm Realm --actionName nextdescendents
```

read

Usage:

```
am> read UserSelfService --realm Realm
```

update

Usage:

```
am> update UserSelfService --realm Realm --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "userRegistration" : {
      "type" : "object",
      "title" : "User Registration",
      "propertyOrder" : 1,
      "properties" : {
        "userRegisteredDestination" : {
          "title" : "Destination After Successful Self-Registration",
```

```
          "description" : "Specifies the action to be taken after a user successfully registers
 a new account. Choose from:<ul><li><code>default</code>. User is sent to a success page without
 being logged in.</li><li><code>login</code>. User is sent to the login page to authenticate.</
li><li><code>autologin</code>. User is automatically logged in and sent to the appropriate page.</
li></ul>",
          "propertyOrder" : 161,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "userRegistrationEnabled" : {
          "title" : "User Registration",
          "description" : "If enabled, new users can sign up for an account.",
          "propertyOrder" : 90,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "userRegistrationEmailVerificationEnabled" : {
          "title" : "Email Verification",
          "description" : "If enabled, users who self-register must perform email address
 verification.",
          "propertyOrder" : 110,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "userRegistrationCaptchaEnabled" : {
          "title" : "Captcha",
          "description" : "If enabled, users must pass a Google reCAPTCHA challenge during user self-
registration to mitigate against software bots.",
          "propertyOrder" : 100,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "userRegistrationEmailBody" : {
          "title" : "Outgoing Email Body",
          "description" : "Customize the User Self-Registration verification email body text. Format
 is: <code>locale|body text</code>.",
          "propertyOrder" : 150,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "userRegistrationEmailSubject" : {
          "title" : "Outgoing Email Subject",
          "description" : "Customize the User Self-Registration verification email subject text.
 Format is <code>locale|subject text</code>.",
          "propertyOrder" : 140,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
```

```
        },
        "userRegistrationKbaEnabled" : {
          "title" : "Security Questions",
          "description" : "If enabled, users must set up their security questions during the self-
registration process.",
          "propertyOrder" : 120,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "userRegistrationValidUserAttributes" : {
          "title" : "Valid Creation Attributes",
          "description" : "Specifies a whitelist of user attributes that can be set during user
 creation.",
          "propertyOrder" : 160,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "userRegistrationEmailVerificationFirstEnabled" : {
          "title" : "Verify Email before User Detail",
          "description" : "If enabled, email address verification will be performed first before user
 details screen is displayed. This will take effect only if Verify Email is enabled.",
          "propertyOrder" : 110,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "userRegistrationTokenTTL" : {
          "title" : "Token Lifetime (seconds)",
          "description" : "Maximum lifetime of the token allowing User Self-Registration, in
 seconds.",
          "propertyOrder" : 130,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        }
      }
    },
    "generalConfig" : {
      "type" : "object",
      "title" : "General Configuration",
      "propertyOrder" : 0,
      "properties" : {
        "validQueryAttributes" : {
          "title" : "Valid Query Attributes",
          "description" : "Specifies the valid query attributes used to search for the user. This is a
 list of attributes used to identify your account for forgotten password and forgotten username.",
          "propertyOrder" : 80,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
```

```
        "captchaVerificationUrl" : {
          "title" : "Google Re-captcha Verification URL",
          "description" : "Google reCAPTCHA plugin verification URL.",
          "propertyOrder" : 40,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "captchaSecretKey" : {
          "title" : "Google reCAPTCHA Secret Key",
          "description" : "Google reCAPTCHA plugin secret key.",
          "propertyOrder" : 30,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "kbaQuestions" : {
          "title" : "Security Questions",
          "description" : "Specifies the default set of knowledge-based authentication (KBA) security
 questions. The security questions can be set for the User Self-Registration, forgotten password
 reset, and forgotten username services, respectively.<p><p>Format is <code>unique key|locale|
question</code>.",
          "propertyOrder" : 50,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "captchaSiteKey" : {
          "title" : "Google reCAPTCHA Site Key",
          "description" : "Google reCAPTCHA plugin site key.",
          "propertyOrder" : 20,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "signingSecretKeyAlias" : {
          "title" : "Signing Secret Key Alias",
          "description" : "A signing secret key alias in the OpenAM server's JCEKS keystore. Used to
 sign the JWT token that OpenAM uses to track end users during User Self-Service operations.",
          "propertyOrder" : 10,
          "required" : true,
          "type" : "string",
          "exampleValue" : "selfservicesigntest"
        },
        "encryptionKeyPairAlias" : {
          "title" : "Encryption Key Pair Alias",
          "description" : "An encryption key alias in the OpenAM server's JCEKS keystore. Used to
 encrypt the JWT token that OpenAM uses to track end users during User Self-Service operations.",
          "propertyOrder" : 0,
          "required" : true,
          "type" : "string",
          "exampleValue" : "selfserviceenctest"
        },
        "minimumAnswersToDefine" : {
          "title" : "Minimum Answers to Define",
          "description" : "Specifies the minimum number of KBA answers that users must define.",
```

```
          "propertyOrder" : 60,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "minimumAnswersToVerify" : {
          "title" : "Minimum Answers to Verify",
          "description" : "Specifies the minimum number of KBA questions that users need to answer
 to be granted the privilege to carry out an action, such as registering for an account, resetting a
 password, or retrieving a username. Specify a value from <code>0</code> to <code>50</code>.",
          "propertyOrder" : 70,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        }
      }
    },
    "advancedConfig" : {
      "type" : "object",
      "title" : "Advanced Configuration",
      "propertyOrder" : 5,
      "properties" : {
        "userRegistrationServiceConfigClass" : {
          "title" : "User Registration Service Config Provider Class",
          "description" : "Specifies the provider class to configure any custom plugins.",
          "propertyOrder" : 350,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "userRegistrationConfirmationUrl" : {
          "title" : "User Registration Confirmation Email URL",
          "description" : "Specifies the confirmation URL that the user receives during the self-
registration process. The <code>${realm}</code> string is replaced with the current realm.",
          "propertyOrder" : 330,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "forgottenPasswordConfirmationUrl" : {
          "title" : "Forgotten Password Confirmation Email URL",
          "description" : "Specifies the confirmation URL that the user receives after confirming
 their identity during the forgotten password process. The <code>${realm}</code> string is replaced
 with the current realm.",
          "propertyOrder" : 340,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "forgottenUsernameServiceConfigClass" : {
          "title" : "Forgotten Username Service Config Provider Class",
          "description" : "Specifies the provider class to configure any custom plugins.",
          "propertyOrder" : 370,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "forgottenPasswordServiceConfigClass" : {
          "title" : "Forgotten Password Service Config Provider Class",
```

```
          "description" : "Specifies the provider class to configure any custom plugins.",
          "propertyOrder" : 360,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "forgottenUsername" : {
      "type" : "object",
      "title" : "Forgotten Username",
      "propertyOrder" : 3,
      "properties" : {
        "forgottenUsernameEnabled" : {
          "title" : "Forgotten Username",
          "description" : "If enabled, users can retrieve their forgotten username.",
          "propertyOrder" : 240,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "forgottenUsernameKbaEnabled" : {
          "title" : "Security Questions",
          "description" : "If enabled, users must answer their security questions during the forgotten
 username process.",
          "propertyOrder" : 260,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "forgottenUsernameEmailSubject" : {
          "title" : "Outgoing Email Subject",
          "description" : "Customizes the forgotten username email subject text. Format is
 <code>locale|subject text</code>.",
          "propertyOrder" : 300,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "forgottenUsernameCaptchaEnabled" : {
          "title" : "Captcha",
          "description" : "If enabled, users must pass a Google reCAPTCHA challenge during the
 forgotten username retrieval process to mitigate against software bots.",
          "propertyOrder" : 250,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "forgottenUsernameEmailBody" : {
          "title" : "Outgoing Email Body",
          "description" : "Customizes the forgotten username email body text. Format is <code>locale|
body text</code>.",
          "propertyOrder" : 310,
          "required" : false,
          "items" : {
            "type" : "string"
```

```
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "forgottenUsernameShowUsernameEnabled" : {
          "title" : "Show Username",
          "description" : "If enabled, users see their forgotten username on the browser page.",
          "propertyOrder" : 280,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "forgottenUsernameTokenTTL" : {
          "title" : "Token LifeTime (seconds)",
          "description" : "Maximum lifetime for the token allowing forgotten username, in seconds.",
          "propertyOrder" : 290,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "forgottenUsernameEmailUsernameEnabled" : {
          "title" : "Email Username",
          "description" : "If enabled, users receive their forgotten username by email.",
          "propertyOrder" : 270,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        }
      }
    },
    "forgottenPassword" : {
      "type" : "object",
      "title" : "Forgotten Password",
      "propertyOrder" : 2,
      "properties" : {
        "forgottenPasswordTokenTTL" : {
          "title" : "Token Lifetime (seconds)",
          "description" : "Maximum lifetime for the token allowing forgotten password reset, in
seconds.<p><p>Specify a value from <code>0</code> to <code>2147483647</code>.",
          "propertyOrder" : 210,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "forgottenPasswordKbaEnabled" : {
          "title" : "Security Questions",
          "description" : "If enabled, users must answer their security questions during the forgotten
password process.",
          "propertyOrder" : 200,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "forgottenPasswordEnabled" : {
          "title" : "Forgotten Password",
          "description" : "If enabled, users can reset their forgotten password.",
          "propertyOrder" : 170,
          "required" : true,
          "type" : "boolean",
```

```
          "exampleValue" : ""
        },
        "forgottenPasswordEmailVerificationEnabled" : {
          "title" : "Email Verification",
          "description" : "If enabled, users who reset passwords must perform email address
 verification.",
          "propertyOrder" : 190,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "forgottenPasswordCaptchaEnabled" : {
          "title" : "Captcha",
          "description" : "If enabled, users must pass a Google reCAPTCHA challenge during password
 reset to mitigate against software bots.",
          "propertyOrder" : 180,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "numberOfAllowedAttempts" : {
          "title" : "Lock Out After number of attempts",
          "description" : "Can be set to 1 or more attempts for a user to correctly answer all their
 security questions. After the number of configured attempts the user has not correctly answered them
 the password reset feature will be disabled.",
          "propertyOrder" : 202,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "forgottenPasswordEmailBody" : {
          "title" : "Outgoing Email Body",
          "description" : "Customize the forgotten password email body text. Format is <code>locale|
body text</code>.",
          "propertyOrder" : 230,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "numberOfAttemptsEnforced" : {
          "title" : "Enforce password reset lockout",
          "description" : "If enabled, users will be prevented from resetting their password after the
 configured number of failed attempts.",
          "propertyOrder" : 201,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "forgottenPasswordEmailSubject" : {
          "title" : "Outgoing Email Subject",
          "description" : "Customize the forgotten password email subject text. Format is
 <code>locale|subject text</code>.",
          "propertyOrder" : 220,
          "required" : false,
          "items" : {
            "type" : "string"
```

```
          },
          "type" : "array",
          "exampleValue" : ""
        }
      }
    },
    "profileManagement" : {
      "type" : "object",
      "title" : "Profile Management",
      "propertyOrder" : 4,
      "properties" : {
        "profileAttributeWhitelist" : {
          "title" : "Self readable attributes",
          "description" : "Specifies the list of attributes that users can view when accessing their
 user profile.",
          "propertyOrder" : 325,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "profileProtectedUserAttributes" : {
          "title" : "Protected Update Attributes",
          "description" : "Specifies a profile's protected user attributes, which causes re-
authentication when the user attempts to modify these attributes.",
          "propertyOrder" : 320,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        }
      }
    }
  }
}
```

Global Operations

Resource path: `/global-config/services/selfService`

Resource version: `1.0`

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action UserSelfService --global --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action UserSelfService --global --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action UserSelfService --global --actionName nextdescendents
```

read

Usage:

```
am> read UserSelfService --global
```

update

Usage:

```
am> update UserSelfService --global --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "defaults" : {
      "properties" : {
        "userRegistration" : {
          "type" : "object",
          "title" : "User Registration",
          "propertyOrder" : 1,
          "properties" : {
            "userRegistrationTokenTTL" : {
              "title" : "Token Lifetime (seconds)",
              "description" : "Maximum lifetime of the token allowing User Self-Registration, in
 seconds.",
              "propertyOrder" : 130,
              "required" : false,
              "type" : "integer",
              "exampleValue" : ""
            },
```

```
            "userRegisteredDestination" : {
              "title" : "Destination After Successful Self-Registration",
              "description" : "Specifies the action to be taken after a user successfully registers
 a new account. Choose from:<ul><li><code>default</code>. User is sent to a success page without
 being logged in.</li><li><code>login</code>. User is sent to the login page to authenticate.</
li><li><code>autologin</code>. User is automatically logged in and sent to the appropriate page.</
li></ul>",
              "propertyOrder" : 161,
              "required" : true,
              "type" : "string",
              "exampleValue" : ""
            },
            "userRegistrationCaptchaEnabled" : {
              "title" : "Captcha",
              "description" : "If enabled, users must pass a Google reCAPTCHA challenge during user
 self-registration to mitigate against software bots.",
              "propertyOrder" : 100,
              "required" : false,
              "type" : "boolean",
              "exampleValue" : ""
            },
            "userRegistrationKbaEnabled" : {
              "title" : "Security Questions",
              "description" : "If enabled, users must set up their security questions during the self-
registration process.",
              "propertyOrder" : 120,
              "required" : false,
              "type" : "boolean",
              "exampleValue" : ""
            },
            "userRegistrationEmailVerificationFirstEnabled" : {
              "title" : "Verify Email before User Detail",
              "description" : "If enabled, email address verification will be performed first before
 user details screen is displayed. This will take effect only if Verify Email is enabled.",
              "propertyOrder" : 110,
              "required" : false,
              "type" : "boolean",
              "exampleValue" : ""
            },
            "userRegistrationValidUserAttributes" : {
              "title" : "Valid Creation Attributes",
              "description" : "Specifies a whitelist of user attributes that can be set during user
 creation.",
              "propertyOrder" : 160,
              "required" : false,
              "items" : {
                "type" : "string"
              },
              "type" : "array",
              "exampleValue" : ""
            },
            "userRegistrationEmailBody" : {
              "title" : "Outgoing Email Body",
              "description" : "Customize the User Self-Registration verification email body text.
 Format is: <code>locale|body text</code>.",
              "propertyOrder" : 150,
              "required" : false,
              "items" : {
                "type" : "string"
```

```
              },
              "type" : "array",
              "exampleValue" : ""
            },
            "userRegistrationEmailVerificationEnabled" : {
              "title" : "Email Verification",
              "description" : "If enabled, users who self-register must perform email address
verification.",
              "propertyOrder" : 110,
              "required" : false,
              "type" : "boolean",
              "exampleValue" : ""
            },
            "userRegistrationEnabled" : {
              "title" : "User Registration",
              "description" : "If enabled, new users can sign up for an account.",
              "propertyOrder" : 90,
              "required" : true,
              "type" : "boolean",
              "exampleValue" : ""
            },
            "userRegistrationEmailSubject" : {
              "title" : "Outgoing Email Subject",
              "description" : "Customize the User Self-Registration verification email subject text.
Format is <code>locale|subject text</code>.",
              "propertyOrder" : 140,
              "required" : false,
              "items" : {
                "type" : "string"
              },
              "type" : "array",
              "exampleValue" : ""
            }
          }
        },
        "forgottenPassword" : {
          "type" : "object",
          "title" : "Forgotten Password",
          "propertyOrder" : 2,
          "properties" : {
            "forgottenPasswordEnabled" : {
              "title" : "Forgotten Password",
              "description" : "If enabled, users can reset their forgotten password.",
              "propertyOrder" : 170,
              "required" : true,
              "type" : "boolean",
              "exampleValue" : ""
            },
            "forgottenPasswordEmailSubject" : {
              "title" : "Outgoing Email Subject",
              "description" : "Customize the forgotten password email subject text. Format is
<code>locale|subject text</code>.",
              "propertyOrder" : 220,
              "required" : false,
              "items" : {
                "type" : "string"
              },
              "type" : "array",
              "exampleValue" : ""
```

```
          },
          "forgottenPasswordKbaEnabled" : {
            "title" : "Security Questions",
            "description" : "If enabled, users must answer their security questions during the
forgotten password process.",
            "propertyOrder" : 200,
            "required" : false,
            "type" : "boolean",
            "exampleValue" : ""
          },
          "forgottenPasswordCaptchaEnabled" : {
            "title" : "Captcha",
            "description" : "If enabled, users must pass a Google reCAPTCHA challenge during
password reset to mitigate against software bots.",
            "propertyOrder" : 180,
            "required" : false,
            "type" : "boolean",
            "exampleValue" : ""
          },
          "forgottenPasswordEmailVerificationEnabled" : {
            "title" : "Email Verification",
            "description" : "If enabled, users who reset passwords must perform email address
verification.",
            "propertyOrder" : 190,
            "required" : false,
            "type" : "boolean",
            "exampleValue" : ""
          },
          "forgottenPasswordTokenTTL" : {
            "title" : "Token Lifetime (seconds)",
            "description" : "Maximum lifetime for the token allowing forgotten password reset, in
seconds.<p><p>Specify a value from <code>0</code> to <code>2147483647</code>.",
            "propertyOrder" : 210,
            "required" : false,
            "type" : "integer",
            "exampleValue" : ""
          },
          "numberOfAttemptsEnforced" : {
            "title" : "Enforce password reset lockout",
            "description" : "If enabled, users will be prevented from resetting their password after
the configured number of failed attempts.",
            "propertyOrder" : 201,
            "required" : false,
            "type" : "boolean",
            "exampleValue" : ""
          },
          "numberOfAllowedAttempts" : {
            "title" : "Lock Out After number of attempts",
            "description" : "Can be set to 1 or more attempts for a user to correctly answer all
their security questions. After the number of configured attempts the user has not correctly answered
them the password reset feature will be disabled.",
            "propertyOrder" : 202,
            "required" : false,
            "type" : "integer",
            "exampleValue" : ""
          },
          "forgottenPasswordEmailBody" : {
            "title" : "Outgoing Email Body",
```

```
              "description" : "Customize the forgotten password email body text. Format is
 <code>locale|body text</code>.",
              "propertyOrder" : 230,
              "required" : false,
              "items" : {
                "type" : "string"
              },
              "type" : "array",
              "exampleValue" : ""
            }
          }
        },
        "advancedConfig" : {
          "type" : "object",
          "title" : "Advanced Configuration",
          "propertyOrder" : 5,
          "properties" : {
            "forgottenUsernameServiceConfigClass" : {
              "title" : "Forgotten Username Service Config Provider Class",
              "description" : "Specifies the provider class to configure any custom plugins.",
              "propertyOrder" : 370,
              "required" : false,
              "type" : "string",
              "exampleValue" : ""
            },
            "userRegistrationServiceConfigClass" : {
              "title" : "User Registration Service Config Provider Class",
              "description" : "Specifies the provider class to configure any custom plugins.",
              "propertyOrder" : 350,
              "required" : false,
              "type" : "string",
              "exampleValue" : ""
            },
            "forgottenPasswordServiceConfigClass" : {
              "title" : "Forgotten Password Service Config Provider Class",
              "description" : "Specifies the provider class to configure any custom plugins.",
              "propertyOrder" : 360,
              "required" : false,
              "type" : "string",
              "exampleValue" : ""
            },
            "userRegistrationConfirmationUrl" : {
              "title" : "User Registration Confirmation Email URL",
              "description" : "Specifies the confirmation URL that the user receives during the self-
registration process. The <code>${realm}</code> string is replaced with the current realm.",
              "propertyOrder" : 330,
              "required" : false,
              "type" : "string",
              "exampleValue" : ""
            },
            "forgottenPasswordConfirmationUrl" : {
              "title" : "Forgotten Password Confirmation Email URL",
              "description" : "Specifies the confirmation URL that the user receives after confirming
 their identity during the forgotten password process. The <code>${realm}</code> string is replaced
 with the current realm.",
              "propertyOrder" : 340,
              "required" : false,
              "type" : "string",
              "exampleValue" : ""
```

```
            }
          }
        },
        "forgottenUsername" : {
          "type" : "object",
          "title" : "Forgotten Username",
          "propertyOrder" : 3,
          "properties" : {
            "forgottenUsernameEnabled" : {
              "title" : "Forgotten Username",
              "description" : "If enabled, users can retrieve their forgotten username.",
              "propertyOrder" : 240,
              "required" : true,
              "type" : "boolean",
              "exampleValue" : ""
            },
            "forgottenUsernameEmailUsernameEnabled" : {
              "title" : "Email Username",
              "description" : "If enabled, users receive their forgotten username by email.",
              "propertyOrder" : 270,
              "required" : false,
              "type" : "boolean",
              "exampleValue" : ""
            },
            "forgottenUsernameCaptchaEnabled" : {
              "title" : "Captcha",
              "description" : "If enabled, users must pass a Google reCAPTCHA challenge during the
forgotten username retrieval process to mitigate against software bots.",
              "propertyOrder" : 250,
              "required" : false,
              "type" : "boolean",
              "exampleValue" : ""
            },
            "forgottenUsernameKbaEnabled" : {
              "title" : "Security Questions",
              "description" : "If enabled, users must answer their security questions during the
forgotten username process.",
              "propertyOrder" : 260,
              "required" : false,
              "type" : "boolean",
              "exampleValue" : ""
            },
            "forgottenUsernameTokenTTL" : {
              "title" : "Token LifeTime (seconds)",
              "description" : "Maximum lifetime for the token allowing forgotten username, in
seconds.",
              "propertyOrder" : 290,
              "required" : false,
              "type" : "integer",
              "exampleValue" : ""
            },
            "forgottenUsernameShowUsernameEnabled" : {
              "title" : "Show Username",
              "description" : "If enabled, users see their forgotten username on the browser page.",
              "propertyOrder" : 280,
              "required" : false,
              "type" : "boolean",
              "exampleValue" : ""
            },
```

```
            "forgottenUsernameEmailSubject" : {
              "title" : "Outgoing Email Subject",
              "description" : "Customizes the forgotten username email subject text. Format is
 <code>locale|subject text</code>.",
              "propertyOrder" : 300,
              "required" : false,
              "items" : {
                "type" : "string"
              },
              "type" : "array",
              "exampleValue" : ""
            },
            "forgottenUsernameEmailBody" : {
              "title" : "Outgoing Email Body",
              "description" : "Customizes the forgotten username email body text. Format is
 <code>locale|body text</code>.",
              "propertyOrder" : 310,
              "required" : false,
              "items" : {
                "type" : "string"
              },
              "type" : "array",
              "exampleValue" : ""
            }
          }
        },
        "generalConfig" : {
          "type" : "object",
          "title" : "General Configuration",
          "propertyOrder" : 0,
          "properties" : {
            "kbaQuestions" : {
              "title" : "Security Questions",
              "description" : "Specifies the default set of knowledge-based authentication (KBA)
 security questions. The security questions can be set for the User Self-Registration, forgotten
 password reset, and forgotten username services, respectively.<p><p>Format is <code>unique key|
locale|question</code>.",
              "propertyOrder" : 50,
              "required" : false,
              "items" : {
                "type" : "string"
              },
              "type" : "array",
              "exampleValue" : ""
            },
            "validQueryAttributes" : {
              "title" : "Valid Query Attributes",
              "description" : "Specifies the valid query attributes used to search for the user.
 This is a list of attributes used to identify your account for forgotten password and forgotten
 username.",
              "propertyOrder" : 80,
              "required" : false,
              "items" : {
                "type" : "string"
              },
              "type" : "array",
              "exampleValue" : ""
            },
            "captchaSiteKey" : {
```

```
              "title" : "Google reCAPTCHA Site Key",
              "description" : "Google reCAPTCHA plugin site key.",
              "propertyOrder" : 20,
              "required" : false,
              "type" : "string",
              "exampleValue" : ""
            },
            "encryptionKeyPairAlias" : {
              "title" : "Encryption Key Pair Alias",
              "description" : "An encryption key alias in the OpenAM server's JCEKS keystore. Used to
encrypt the JWT token that OpenAM uses to track end users during User Self-Service operations.",
              "propertyOrder" : 0,
              "required" : true,
              "type" : "string",
              "exampleValue" : "selfserviceenctest"
            },
            "signingSecretKeyAlias" : {
              "title" : "Signing Secret Key Alias",
              "description" : "A signing secret key alias in the OpenAM server's JCEKS keystore. Used
to sign the JWT token that OpenAM uses to track end users during User Self-Service operations.",
              "propertyOrder" : 10,
              "required" : true,
              "type" : "string",
              "exampleValue" : "selfservicesigntest"
            },
            "minimumAnswersToVerify" : {
              "title" : "Minimum Answers to Verify",
              "description" : "Specifies the minimum number of KBA questions that users need to answer
to be granted the privilege to carry out an action, such as registering for an account, resetting a
password, or retrieving a username. Specify a value from <code>0</code> to <code>50</code>.",
              "propertyOrder" : 70,
              "required" : false,
              "type" : "integer",
              "exampleValue" : ""
            },
            "captchaSecretKey" : {
              "title" : "Google reCAPTCHA Secret Key",
              "description" : "Google reCAPTCHA plugin secret key.",
              "propertyOrder" : 30,
              "required" : false,
              "type" : "string",
              "exampleValue" : ""
            },
            "minimumAnswersToDefine" : {
              "title" : "Minimum Answers to Define",
              "description" : "Specifies the minimum number of KBA answers that users must define.",
              "propertyOrder" : 60,
              "required" : false,
              "type" : "integer",
              "exampleValue" : ""
            },
            "captchaVerificationUrl" : {
              "title" : "Google Re-captcha Verification URL",
              "description" : "Google reCAPTCHA plugin verification URL.",
              "propertyOrder" : 40,
              "required" : false,
              "type" : "string",
              "exampleValue" : ""
            }
```

```
          }
        },
        "profileManagement" : {
          "type" : "object",
          "title" : "Profile Management",
          "propertyOrder" : 4,
          "properties" : {
            "profileAttributeWhitelist" : {
              "title" : "Self readable attributes",
              "description" : "Specifies the list of attributes that users can view when accessing
 their user profile.",
              "propertyOrder" : 325,
              "required" : false,
              "items" : {
                "type" : "string"
              },
              "type" : "array",
              "exampleValue" : ""
            },
            "profileProtectedUserAttributes" : {
              "title" : "Protected Update Attributes",
              "description" : "Specifies a profile's protected user attributes, which causes re-
authentication when the user attempts to modify these attributes.",
              "propertyOrder" : 320,
              "required" : false,
              "items" : {
                "type" : "string"
              },
              "type" : "array",
              "exampleValue" : ""
            }
          }
        }
      },
      "type" : "object",
      "title" : "Realm Defaults"
    }
  }
}
```

UserServices

Realm Operations

Resource path: `/users/{user}/services`

Resource version: `1.0`

create

Usage:

```
am> create UserServices --realm Realm --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object"
}
```

delete

Usage:

```
am> delete UserServices --realm Realm
```

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action UserServices --realm Realm --user user --actionName getAllTypes
```

Parameters:

--user

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action UserServices --realm Realm --user user --actionName getCreatableTypes
```

Parameters:

--user

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action UserServices --realm Realm --user user --actionName nextdescendents
```

Parameters:

--user

read

Usage:

```
am> read UserServices --realm Realm
```

unassignServices

action.unassignServices.description

Usage:

```
am> action UserServices --realm Realm --body body --user user --actionName unassignServices
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "description" : "i18n:api-descriptor/UserServicesResource#schema.description",
  "type" : "object",
  "title" : "i18n:api-descriptor/UserServicesResource#schema.title",
  "properties" : {
    "serviceNames" : {
      "type" : "array",
      "title" : "i18n:api-descriptor/UserServicesResource#schema.servicename.title",
      "description" : "i18n:api-descriptor/UserServicesResource#schema.servicename.description",
      "items" : {
        "type" : "string"
      }
    }
  }
}
```

--user

update

Usage:

```
am> update UserServices --realm Realm --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object"
}
```

UsernameCollector

Realm Operations

Resource path: `/realm-config/authentication/authenticationtrees/nodes/UsernameCollectorNode`

Resource version: `1.0`

create

Usage:

```
am> create UsernameCollector --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "required" : [ ]
}
```

delete

Usage:

```
am> delete UsernameCollector --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action UsernameCollector --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action UsernameCollector --realm Realm --actionName getCreatableTypes
```

listOutcomes

List the available outcomes for the node type.

Usage:

```
am> action UsernameCollector --realm Realm --body body --actionName listOutcomes
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "title" : "Some configuration of the node. This does not need to be complete against the
 configuration schema."
}
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action UsernameCollector --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query UsernameCollector --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read UsernameCollector --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update UsernameCollector --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "required" : [ ]
}
```

VKClient

Realm Operations

Resource path: `/realm-config/services/SocialIdentityProviders/vkConfig`

Resource version: `1.0`

create

Usage:

```
am> create VKClient --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "userInfoEndpoint" : {
      "title" : "User Profile Service URL",
      "description" : "User profile information URL <p> This URL endpoint provides user profile
 information and is provided by the OAuth Identity Provider NB This URL should return JSON objects in
 response.",
      "propertyOrder" : 600,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "apiVersion" : {
      "title" : "API Version",
      "description" : "Version of the applicable VKontakte API.",
      "propertyOrder" : 1200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "scopeDelimiter" : {
      "title" : "Scope Delimiter",
      "description" : "The delimiter used by an auth server to separate scopes.",
      "propertyOrder" : 800,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "clientId" : {
      "title" : "Client ID",
      "description" : "OAuth client_id parameter<p> For more information on the OAuth client_id
 parameter refer to the RFC 6749 (http://tools.ietf.org/html/rfc6749#section-2.3.1), section 2.3.1.",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "redirectURI" : {
      "title" : "Redirect URL",
      "description" : "",
      "propertyOrder" : 700,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
```

```
    },
    "pkceMethod" : {
      "title" : "PKCE Method",
      "description" : "The PKCE transformation method to use when making requests to the authorization
 endpoint.",
      "propertyOrder" : 1100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "tokenEndpoint" : {
      "title" : "Access Token Endpoint URL",
      "description" : "OAuth access token endpoint URL This is the URL endpoint for access token
 retrieval provided by the OAuth Identity Provider.Refer to the RFC 6749 (http://tools.ietf.org/html/
rfc6749#section-3.2), section 3.2.",
      "propertyOrder" : 500,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "basicAuth" : {
      "title" : "Use Basic Auth",
      "description" : "When enabled, the client will use basic auth for authenticating with the social
 auth provider. Enabled by default.",
      "propertyOrder" : 1000,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "clientSecret" : {
      "title" : "Client Secret",
      "description" : "OAuth client_secret parameter <p>For more information on the OAuth client_id
 parameter refer to the RFC 6749 (http://tools.ietf.org/html/rfc6749#section-2.3.1), section 2.3.1.",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "string",
      "format" : "password",
      "exampleValue" : ""
    },
    "authenticationIdKey" : {
      "title" : "Auth ID Key",
      "description" : "Field used to identify a user by the social provider.",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "exampleValue" : "sub"
    },
    "transform" : {
      "title" : "Transform Script",
      "description" : "A script that takes the raw profile object as input and outputs the normalized
 profile object.",
      "propertyOrder" : 10000,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "authorizationEndpoint" : {
      "title" : "Authentication Endpoint URL",
```

```
      "description" : "OAuth authentication endpoint URL <p> This is the URL endpoint for OAuth
 authentication provided by the OAuth Identity Provider.",
      "propertyOrder" : 400,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "scopes" : {
      "title" : "OAuth Scopes",
      "description" : "List of user profile properties<p>According to the OAuth 2.0 Authorization
 Framework that the client application requires. The list depends on the permissions that the resource
 owner grants to the client application. Some authorization servers use non-standard separators for
 scopes.",
      "propertyOrder" : 900,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "minItems" : 1,
      "type" : "array",
      "exampleValue" : ""
    },
    "uiConfig" : {
      "title" : "UI Config Properties",
      "description" : "Mapping of display properties to be defined and consumed by the UI.",
      "propertyOrder" : 9999,
      "required" : true,
      "patternProperties" : {
        ".*" : {
          "type" : "string"
        }
      },
      "type" : "object",
      "exampleValue" : ""
    },
    "enabled" : {
      "title" : "Enabled",
      "description" : "",
      "propertyOrder" : 1,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    }
  }
}
```

delete

Usage:

```
am> delete VKClient --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action VKClient --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action VKClient --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action VKClient --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query VKClient --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read VKClient --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update VKClient --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "userInfoEndpoint" : {
      "title" : "User Profile Service URL",
      "description" : "User profile information URL <p> This URL endpoint provides user profile
 information and is provided by the OAuth Identity Provider NB This URL should return JSON objects in
 response.",
      "propertyOrder" : 600,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "apiVersion" : {
      "title" : "API Version",
      "description" : "Version of the applicable VKontakte API.",
      "propertyOrder" : 1200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "scopeDelimiter" : {
      "title" : "Scope Delimiter",
      "description" : "The delimiter used by an auth server to separate scopes.",
      "propertyOrder" : 800,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "clientId" : {
      "title" : "Client ID",
      "description" : "OAuth client_id parameter<p> For more information on the OAuth client_id
 parameter refer to the RFC 6749 (http://tools.ietf.org/html/rfc6749#section-2.3.1), section 2.3.1.",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
```

```
      "exampleValue" : ""
    },
    "redirectURI" : {
      "title" : "Redirect URL",
      "description" : "",
      "propertyOrder" : 700,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "pkceMethod" : {
      "title" : "PKCE Method",
      "description" : "The PKCE transformation method to use when making requests to the authorization
 endpoint.",
      "propertyOrder" : 1100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "tokenEndpoint" : {
      "title" : "Access Token Endpoint URL",
      "description" : "OAuth access token endpoint URL This is the URL endpoint for access token
 retrieval provided by the OAuth Identity Provider.Refer to the RFC 6749 (http://tools.ietf.org/html/
rfc6749#section-3.2), section 3.2.",
      "propertyOrder" : 500,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "basicAuth" : {
      "title" : "Use Basic Auth",
      "description" : "When enabled, the client will use basic auth for authenticating with the social
 auth provider. Enabled by default.",
      "propertyOrder" : 1000,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "clientSecret" : {
      "title" : "Client Secret",
      "description" : "OAuth client_secret parameter <p>For more information on the OAuth client_id
 parameter refer to the RFC 6749 (http://tools.ietf.org/html/rfc6749#section-2.3.1), section 2.3.1.",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "string",
      "format" : "password",
      "exampleValue" : ""
    },
    "authenticationIdKey" : {
      "title" : "Auth ID Key",
      "description" : "Field used to identify a user by the social provider.",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "exampleValue" : "sub"
    },
    "transform" : {
      "title" : "Transform Script",
```

```
      "description" : "A script that takes the raw profile object as input and outputs the normalized
 profile object.",
      "propertyOrder" : 10000,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "authorizationEndpoint" : {
      "title" : "Authentication Endpoint URL",
      "description" : "OAuth authentication endpoint URL <p> This is the URL endpoint for OAuth
 authentication provided by the OAuth Identity Provider.",
      "propertyOrder" : 400,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "scopes" : {
      "title" : "OAuth Scopes",
      "description" : "List of user profile properties<p>According to the OAuth 2.0 Authorization
 Framework that the client application requires. The list depends on the permissions that the resource
 owner grants to the client application. Some authorization servers use non-standard separators for
 scopes.",
      "propertyOrder" : 900,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "minItems" : 1,
      "type" : "array",
      "exampleValue" : ""
    },
    "uiConfig" : {
      "title" : "UI Config Properties",
      "description" : "Mapping of display properties to be defined and consumed by the UI.",
      "propertyOrder" : 9999,
      "required" : true,
      "patternProperties" : {
        ".*" : {
          "type" : "string"
        }
      },
      "type" : "object",
      "exampleValue" : ""
    },
    "enabled" : {
      "title" : "Enabled",
      "description" : "",
      "propertyOrder" : 1,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    }
  }
}
```

ValidationService

Realm Operations

Resource path: `/realm-config/services/validation`

Resource version: `1.0`

create

Usage:

```
am> create ValidationService --realm Realm --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "validGotoDestinations" : {
      "title" : "Valid goto URL Resources",
      "description" : "List of valid goto URL resources.<br><br>Specifies a list of valid URLs for
 the <code>goto</code> and <code>gotoOnFail</code> query string parameters. AM only redirects a user
 after log in or log out to a URL in this list. If the URL is not in the list, AM redirects to either
 the user profile page, or the administration console. If this property is not set, AM will only allow
 URLs that match its domain; for example, <code>domain-of-am-instance.com</code>. Use the <code>*</
code> wildcard to match all characters except <code>?</code>.<p> Examples: </p> <ul><li><code>http://
app.example.com:80/*</code></li> <li><code>http://app.example.com:80/*?*</code></li></ul>",
      "propertyOrder" : 100,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    }
  }
}
```

delete

Usage:

```
am> delete ValidationService --realm Realm
```

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action ValidationService --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action ValidationService --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action ValidationService --realm Realm --actionName nextdescendents
```

read

Usage:

```
am> read ValidationService --realm Realm
```

update

Usage:

```
am> update ValidationService --realm Realm --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "validGotoDestinations" : {
      "title" : "Valid goto URL Resources",
      "description" : "List of valid goto URL resources.<br><br>Specifies a list of valid URLs for
 the <code>goto</code> and <code>gotoOnFail</code> query string parameters. AM only redirects a user
 after log in or log out to a URL in this list. If the URL is not in the list, AM redirects to either
 the user profile page, or the administration console. If this property is not set, AM will only allow
 URLs that match its domain; for example, <code>domain-of-am-instance.com</code>. Use the <code>*</
code> wildcard to match all characters except <code>?</code>.<p> Examples: </p> <ul><li><code>http://
app.example.com:80/*</code></li> <li><code>http://app.example.com:80/*?*</code></li></ul>",
      "propertyOrder" : 100,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    }
  }
}
```


Global Operations

Resource path: `/global-config/services/validation`

Resource version: `1.0`

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action ValidationService --global --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action ValidationService --global --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action ValidationService --global --actionName nextdescendents
```

read

Usage:

```
am> read ValidationService --global
```

update

Usage:

```
am> update ValidationService --global --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "defaults" : {
      "properties" : {
        "validGotoDestinations" : {
          "title" : "Valid goto URL Resources",
          "description" : "List of valid goto URL resources.<br><br>Specifies a list of valid URLs for
 the <code>goto</code> and <code>gotoOnFail</code> query string parameters. AM only redirects a user
 after log in or log out to a URL in this list. If the URL is not in the list, AM redirects to either
 the user profile page, or the administration console. If this property is not set, AM will only allow
 URLs that match its domain; for example, <code>domain-of-am-instance.com</code>. Use the <code>*</
code> wildcard to match all characters except <code>?</code>.<p> Examples: </p> <ul><li><code>http://
app.example.com:80/*</code></li> <li><code>http://app.example.com:80/*?*</code></li></ul>",
          "propertyOrder" : 100,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        }
      },
      "type" : "object",
      "title" : "Realm Defaults"
    }
  }
}
```

WeChatClient

Realm Operations

Resource path: `/realm-config/services/SocialIdentityProviders/weChatConfig`

Resource version: `1.0`

create

Usage:

```
am> create WeChatClient --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "authenticationIdKey" : {
      "title" : "Auth ID Key",
      "description" : "Field used to identify a user by the social provider.",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "exampleValue" : "sub"
    },
    "pkceMethod" : {
      "title" : "PKCE Method",
      "description" : "The PKCE transformation method to use when making requests to the authorization
 endpoint.",
      "propertyOrder" : 1100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "redirectURI" : {
      "title" : "Redirect URL",
      "description" : "",
      "propertyOrder" : 700,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "scopes" : {
```

```
     "title" : "OAuth Scopes",
     "description" : "List of user profile properties<p>According to the OAuth 2.0 Authorization
Framework that the client application requires. The list depends on the permissions that the resource
owner grants to the client application. Some authorization servers use non-standard separators for
scopes.",
     "propertyOrder" : 900,
     "required" : true,
     "items" : {
       "type" : "string"
     },
     "minItems" : 1,
     "type" : "array",
     "exampleValue" : ""
   },
   "clientSecret" : {
     "title" : "Client Secret",
     "description" : "OAuth client_secret parameter <p>For more information on the OAuth client_id
parameter refer to the RFC 6749 (http://tools.ietf.org/html/rfc6749#section-2.3.1), section 2.3.1.",
     "propertyOrder" : 300,
     "required" : true,
     "type" : "string",
     "format" : "password",
     "exampleValue" : ""
   },
   "userInfoEndpoint" : {
     "title" : "User Profile Service URL",
     "description" : "User profile information URL <p> This URL endpoint provides user profile
information and is provided by the OAuth Identity Provider NB This URL should return JSON objects in
response.",
     "propertyOrder" : 600,
     "required" : true,
     "type" : "string",
     "exampleValue" : ""
   },
   "scopeDelimiter" : {
     "title" : "Scope Delimiter",
     "description" : "The delimiter used by an auth server to separate scopes.",
     "propertyOrder" : 800,
     "required" : true,
     "type" : "string",
     "exampleValue" : ""
   },
   "clientId" : {
     "title" : "Client ID",
     "description" : "OAuth client_id parameter<p> For more information on the OAuth client_id
parameter refer to the RFC 6749 (http://tools.ietf.org/html/rfc6749#section-2.3.1), section 2.3.1.",
     "propertyOrder" : 200,
     "required" : true,
     "type" : "string",
     "exampleValue" : ""
   },
   "uiConfig" : {
     "title" : "UI Config Properties",
     "description" : "Mapping of display properties to be defined and consumed by the UI.",
     "propertyOrder" : 9999,
     "required" : true,
     "patternProperties" : {
       ".*" : {
         "type" : "string"
```

```
        }
      },
      "type" : "object",
      "exampleValue" : ""
    },
    "enabled" : {
      "title" : "Enabled",
      "description" : "",
      "propertyOrder" : 1,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "authorizationEndpoint" : {
      "title" : "Authentication Endpoint URL",
      "description" : "OAuth authentication endpoint URL <p> This is the URL endpoint for OAuth
 authentication provided by the OAuth Identity Provider.",
      "propertyOrder" : 400,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "refreshTokenEndpoint" : {
      "title" : "Refresh Token Endpoint",
      "description" : "The endpoint for obtaining a refresh token.",
      "propertyOrder" : 1200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "basicAuth" : {
      "title" : "Use Basic Auth",
      "description" : "When enabled, the client will use basic auth for authenticating with the social
 auth provider. Enabled by default.",
      "propertyOrder" : 1000,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "transform" : {
      "title" : "Transform Script",
      "description" : "A script that takes the raw profile object as input and outputs the normalized
 profile object.",
      "propertyOrder" : 10000,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "tokenEndpoint" : {
      "title" : "Access Token Endpoint URL",
      "description" : "OAuth access token endpoint URL This is the URL endpoint for access token
 retrieval provided by the OAuth Identity Provider.Refer to the RFC 6749 (http://tools.ietf.org/html/
rfc6749#section-3.2), section 3.2.",
      "propertyOrder" : 500,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }
```

```
}
```

delete

Usage:

```
am> delete WeChatClient --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action WeChatClient --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action WeChatClient --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action WeChatClient --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query WeChatClient --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read WeChatClient --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update WeChatClient --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "authenticationIdKey" : {
      "title" : "Auth ID Key",
      "description" : "Field used to identify a user by the social provider.",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "exampleValue" : "sub"
    },
    "pkceMethod" : {
      "title" : "PKCE Method",
      "description" : "The PKCE transformation method to use when making requests to the authorization
 endpoint.",
      "propertyOrder" : 1100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "redirectURI" : {
      "title" : "Redirect URL",
```

```
     "description" : "",
     "propertyOrder" : 700,
     "required" : true,
     "type" : "string",
     "exampleValue" : ""
   },
   "scopes" : {
     "title" : "OAuth Scopes",
     "description" : "List of user profile properties<p>According to the OAuth 2.0 Authorization
Framework that the client application requires. The list depends on the permissions that the resource
owner grants to the client application. Some authorization servers use non-standard separators for
scopes.",
     "propertyOrder" : 900,
     "required" : true,
     "items" : {
       "type" : "string"
     },
     "minItems" : 1,
     "type" : "array",
     "exampleValue" : ""
   },
   "clientSecret" : {
     "title" : "Client Secret",
     "description" : "OAuth client_secret parameter <p>For more information on the OAuth client_id
parameter refer to the RFC 6749 (http://tools.ietf.org/html/rfc6749#section-2.3.1), section 2.3.1.",
     "propertyOrder" : 300,
     "required" : true,
     "type" : "string",
     "format" : "password",
     "exampleValue" : ""
   },
   "userInfoEndpoint" : {
     "title" : "User Profile Service URL",
     "description" : "User profile information URL <p> This URL endpoint provides user profile
information and is provided by the OAuth Identity Provider NB This URL should return JSON objects in
response.",
     "propertyOrder" : 600,
     "required" : true,
     "type" : "string",
     "exampleValue" : ""
   },
   "scopeDelimiter" : {
     "title" : "Scope Delimiter",
     "description" : "The delimiter used by an auth server to separate scopes.",
     "propertyOrder" : 800,
     "required" : true,
     "type" : "string",
     "exampleValue" : ""
   },
   "clientId" : {
     "title" : "Client ID",
     "description" : "OAuth client_id parameter<p> For more information on the OAuth client_id
parameter refer to the RFC 6749 (http://tools.ietf.org/html/rfc6749#section-2.3.1), section 2.3.1.",
     "propertyOrder" : 200,
     "required" : true,
     "type" : "string",
     "exampleValue" : ""
   },
   "uiConfig" : {
```

```
      "title" : "UI Config Properties",
      "description" : "Mapping of display properties to be defined and consumed by the UI.",
      "propertyOrder" : 9999,
      "required" : true,
      "patternProperties" : {
        ".*" : {
          "type" : "string"
        }
      },
      "type" : "object",
      "exampleValue" : ""
    },
    "enabled" : {
      "title" : "Enabled",
      "description" : "",
      "propertyOrder" : 1,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "authorizationEndpoint" : {
      "title" : "Authentication Endpoint URL",
      "description" : "OAuth authentication endpoint URL <p> This is the URL endpoint for OAuth
authentication provided by the OAuth Identity Provider.",
      "propertyOrder" : 400,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "refreshTokenEndpoint" : {
      "title" : "Refresh Token Endpoint",
      "description" : "The endpoint for obtaining a refresh token.",
      "propertyOrder" : 1200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "basicAuth" : {
      "title" : "Use Basic Auth",
      "description" : "When enabled, the client will use basic auth for authenticating with the social
auth provider. Enabled by default.",
      "propertyOrder" : 1000,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "transform" : {
      "title" : "Transform Script",
      "description" : "A script that takes the raw profile object as input and outputs the normalized
profile object.",
      "propertyOrder" : 10000,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "tokenEndpoint" : {
      "title" : "Access Token Endpoint URL",
```

```
      "description" : "OAuth access token endpoint URL This is the URL endpoint for access token
 retrieval provided by the OAuth Identity Provider.Refer to the RFC 6749 (http://tools.ietf.org/html/
rfc6749#section-3.2), section 3.2.",
      "propertyOrder" : 500,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
```

WebAgentGroups

Realm Operations

Agent Groups handler that is responsible for managing agent groups

Resource path: `/realm-config/agents/groups/WebAgent`

Resource version: `1.0`

create

Usage:

```
am> create WebAgentGroups --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "applicationWebAgentConfig" : {
      "type" : "object",
      "title" : "Application",
      "propertyOrder" : 1,
      "properties" : {
        "continuousSecurityCookies" : {
          "title" : "Continuous Security Cookies",
          "description" : "The name of the cookies to be sent as part of the payload during policy
 evaluation, which can be accessed via the 'environment' variable in a policy script. The 'key' is
 the name of the cookie to be sent, and the 'value' is the name which it will appear as in the policy
 evaluation script. It is possible to map multiple cookies to the same name (they will simply appear
```

```
as an array in the evaluation script). If the cookie doesn't exist, then the empty string will be
sent.",
         "propertyOrder" : 28900,
         "required" : false,
         "patternProperties" : {
           ".*" : {
             "type" : "string"
           }
         },
         "type" : "object",
         "exampleValue" : ""
       },
       "profileAttributeFetchMode" : {
         "title" : "Profile Attribute Fetch Mode",
         "description" : "(property name:
com.sun.identity.agents.config.profile.attribute.fetch.mode)",
         "propertyOrder" : 28200,
         "required" : false,
         "type" : "string",
         "exampleValue" : ""
       },
       "notEnforcedIpsRegex" : {
         "title" : "Regular Expressions for Not-Enforced IPs",
         "description" : "Enable use of Perl-compatible regular expressions in Not-Enforced URL from
IP settings. (property: org.forgerock.agents.config.notenforced.ext.regex.enable)",
         "propertyOrder" : 28150,
         "required" : false,
         "type" : "boolean",
         "exampleValue" : ""
       },
       "sessionAttributeFetchMode" : {
         "title" : "Session Attribute Fetch Mode",
         "description" : "(property name:
com.sun.identity.agents.config.session.attribute.fetch.mode)",
         "propertyOrder" : 28600,
         "required" : false,
         "type" : "string",
         "exampleValue" : ""
       },
       "continuousSecurityHeaders" : {
         "title" : "Continuous Security Headers",
         "description" : "The name of the headers in the user's original request, that will be sent
as part of the payload during policy evaluation, which can then be accessed via the 'environment'
variable in a policy script. The 'key' is the name of the header to be sent, and the 'value' is the
name which it will appear as in the policy evaluation script.It is possible to map multiple headers
to the same name (they will simply appear as an array in the evaluation script). If the header
doesn't exist, then the empty string will be sent.",
         "propertyOrder" : 29000,
         "required" : false,
         "patternProperties" : {
           ".*" : {
             "type" : "string"
           }
         },
         "type" : "object",
         "exampleValue" : ""
       },
       "notEnforcedIpsList" : {
         "title" : "Not-Enforced URL from IP Processing List",
```

```
          "description" : "Specifies a list of client IP addresses that do not require authentication
 when requesting the indicated URLs. <br>The supported format requires a list of IP addresses
 separated by spaces, the horizontal bar (|) character, and a list of URLs separated by spaces.
 <br>For example: <br>  10.1.2.1 192.168.0.2|/public/* <br>In the preceding example, the IP addresses
 10.1.2.1 and  192.168.0.2 can access any resource inside /public without authenticating. (property:
 org.forgerock.agents.config.notenforced.ipurl)",
          "propertyOrder" : 28050,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "notEnforcedUrlsRegex" : {
          "title" : "Regular Expressions for Not-Enforced URLs",
          "description" : "When true, enables use of Perl-compatible regular expressions in Not-
enforced URL settings. (property: com.forgerock.agents.notenforced.url.regex.enable)",
          "propertyOrder" : 27850,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "sessionAttributeMap" : {
          "title" : "Session Attribute Map",
          "description" : "Maps the session attributes to be populated
 under specific names for the currently authenticated user. (property name:
 com.sun.identity.agents.config.session.attribute.mapping)   <br> Example: <br>  To populate the value
 of session attribute UserToken under name CUSTOM-userid: enter UserToken in Map Key field, and enter
 CUSTOM-userid in Corresponding Map Value field.",
          "propertyOrder" : 28700,
          "required" : false,
          "patternProperties" : {
            ".*" : {
              "type" : "string"
            }
          },
          "type" : "object",
          "exampleValue" : ""
        },
        "responseAttributeMap" : {
          "title" : "Response Attribute Map",
          "description" : "Maps the policy response attributes to be populated
 under specific names for the currently authenticated user. (property name:
 com.sun.identity.agents.config.response.attribute.mapping)  <br> Example: <br> To populate the value
 of response attribute uid under name CUSTOM-USER-NAME: enter uid in Map Key field, and enter CUSTOM-
USER-NAME in Corresponding Map Value field.",
          "propertyOrder" : 28500,
          "required" : false,
          "patternProperties" : {
            ".*" : {
              "type" : "string"
            }
          },
          "type" : "object",
          "exampleValue" : ""
        },
        "profileAttributeMap" : {
          "title" : "Profile Attribute Map",
```

```
          "description" : "Maps the profile attributes to be populated
 under specific names for the currently authenticated user. (property name:
 com.sun.identity.agents.config.profile.attribute.mapping)  <br> Example: <br> To populate the value
 of profile attribute cn under name CUSTOM-Common-Name: enter cn in Map Key field, and enter CUSTOM-
Common-Name in Corresponding Map Value field. <br> To populate the value of profile attribute mail
 under name CUSTOM-Email: enter mail in Map Key field, and enter CUSTOM-Email in Corresponding Map
 Value field.",
          "propertyOrder" : 28300,
          "required" : false,
          "patternProperties" : {
            ".*" : {
              "type" : "string"
            }
          },
          "type" : "object",
          "exampleValue" : ""
        },
        "fetchAttributesForNotEnforcedUrls" : {
          "title" : "Fetch Attributes for Not Enforced URLs",
          "description" : "Agent fetches profile attributes for not enforced urls by doing policy
 evaluation. (property name: com.sun.identity.agents.config.notenforced.url.attributes.enable)",
          "propertyOrder" : 27900,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "attributeMultiValueSeparator" : {
          "title" : "Attribute Multi Value Separator",
          "description" : "Specifies separator for multiple values. Applies to all
 types of attributes i.e. profile, session and response attributes. (property name:
 com.sun.identity.agents.config.attribute.multi.value.separator)",
          "propertyOrder" : 28800,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "invertNotEnforcedUrls" : {
          "title" : "Invert Not Enforced URLs",
          "description" : "Only not enforced list of urls will be enforced. (property name:
 com.sun.identity.agents.config.notenforced.url.invert)",
          "propertyOrder" : 27800,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "ignorePathInfoForNotEnforcedUrls" : {
          "title" : "Ignore Path Info for Not Enforced URLs",
          "description" : "Indicate whether the path info and query should be
 stripped from the request URL before being compared with the URLs of the not
 enforced list when those URLs have a wildcard '*' character.  (property name:
 com.sun.identity.agents.config.ignore.path.info.for.not.enforced.list)  ",
          "propertyOrder" : 27600,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "responseAttributeFetchMode" : {
          "title" : "Response Attribute Fetch Mode",
```

```
          "description" : "(property name:
 com.sun.identity.agents.config.response.attribute.fetch.mode)",
          "propertyOrder" : 28400,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "notEnforcedIps" : {
          "title" : "Not Enforced Client IP List",
          "description" : "No authentication and authorization are required for the requests coming
 from these client IP addresses. (property name: com.sun.identity.agents.config.notenforced.ip) <br>
 Examples: <br> 192.18.145.* <br> 192.18.146.123",
          "propertyOrder" : 28000,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "notEnforcedUrls" : {
          "title" : "Not Enforced URLs",
          "description" : "List of urls for which no authentication required. (property name:
 com.sun.identity.agents.config.notenforced.url) <br> Example: <br> http://myagent.mydomain.com/
*.gif",
          "propertyOrder" : 27700,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "clientIpValidation" : {
          "title" : "Client IP Validation",
          "description" : "This validates if the subsequent browser requests come from
 the same ip address that the SSO token is initially issued against. (property name:
 com.sun.identity.agents.config.client.ip.validation.enable)",
          "propertyOrder" : 28100,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        }
      }
    },
    "globalWebAgentConfig" : {
      "type" : "object",
      "title" : "Global",
      "propertyOrder" : 0,
      "properties" : {
        "agentConfigChangeNotificationsEnabled" : {
          "title" : "Agent Configuration Change Notification",
          "description" : "Enable agent to receive notification messages
 (via websockets) from AM server for configuration changes. (property name:
 org.forgerock.agents.config.change.notifications.enabled) ",
          "propertyOrder" : 25300,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
```

```
      },
      "status" : {
        "title" : "Status",
        "description" : "Status of the agent configuration.",
        "propertyOrder" : 25100,
        "required" : true,
        "type" : "string",
        "exampleValue" : ""
      },
      "jwtName" : {
        "title" : "JWT Cookie Name",
        "description" : "The name used by the agent to set the OIDC JWT on the user's browser.
(property: org.forgerock.agents.jwt.cookie.name)",
        "propertyOrder" : 25500,
        "required" : false,
        "type" : "string",
        "exampleValue" : ""
      },
      "jwtAuditWhitelist" : {
        "title" : "Agent Profile ID Whitelist",
        "description" : "Specifies a comma-separated list of profile IDs that the agent will
consider as valid values for the aud claim. This claim is represented in the JWT containing
the end user's session. <br>Example: <br>agentprofile1,agentprofile2,.... <br>When several
agents configured with different agent profiles protect the same application, set this property
to a list of the agent profiles that are protecting the same application. <br>(property:
com.forgerock.agents.jwt.aud.whitelist)",
        "propertyOrder" : 25520,
        "required" : false,
        "type" : "string",
        "exampleValue" : ""
      },
      "fqdnCheck" : {
        "title" : "FQDN Check",
        "description" : "Enables checking of fqdn default value and fqdn map values. (property name:
com.sun.identity.agents.config.fqdn.check.enable)",
        "propertyOrder" : 27300,
        "required" : false,
        "type" : "boolean",
        "exampleValue" : ""
      },
      "fqdnDefault" : {
        "title" : "FQDN Default",
        "description" : "Fully qualified hostname that the users should use in order to access
resources. (property name: com.sun.identity.agents.config.fqdn.default)",
        "propertyOrder" : 27400,
        "required" : false,
        "type" : "string",
        "exampleValue" : ""
      },
      "accessDeniedUrl" : {
        "title" : "Resources Access Denied URL",
        "description" : "The URL of the customized access denied page. (property name:
com.sun.identity.agents.config.access.denied.url)",
        "propertyOrder" : 26300,
        "required" : false,
        "type" : "string",
        "exampleValue" : ""
      },
      "agentUriPrefix" : {
```

```
          "title" : "Agent Deployment URI Prefix",
          "description" : "(property name: com.sun.identity.agents.config.agenturi.prefix)",
          "propertyOrder" : 25800,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "disableJwtAudit" : {
          "title" : "Disable validation of the audience claim",
          "description" : "Specifies whether the agent should validate the audience claim matches the
agent profile ID represented in the JWT containing the end user's session. <br>Possible values are:
<br>  false = The agent validates audience claim. <br>  true = The agent does not validate audience
claim.<br> (property: com.forgerock.agents.jwt.aud.disable)",
          "propertyOrder" : 25510,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "agentDebugLevel" : {
          "title" : "Agent Debug Level",
          "description" : "Agent debug level. (property name:
com.sun.identity.agents.config.debug.level)",
          "propertyOrder" : 26400,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "fqdnMapping" : {
          "title" : "FQDN Virtual Host Map",
          "description" : "Maps virtual, invalid, or partial hostnames, and IP addresses to the FQDN
to access protected resources. (property name: com.sun.identity.agents.config.fqdn.mapping) <br>
Examples: <br>  To map the partial hostname myserver to myserver.mydomain.com: enter myserver in the
Map Key field and myserver.mydomain.com in the Corresponding Map Value field. To map a virtual server
rst.hostname.com that points to the actual server abc.hostname.com: enter valid1 in the Map Key field
and rst.hostname.com in the Corresponding Map Value field.",
          "propertyOrder" : 27500,
          "required" : false,
          "patternProperties" : {
            ".*" : {
              "type" : "string"
            }
          },
          "type" : "object",
          "exampleValue" : ""
        },
        "configurationPollingInterval" : {
          "title" : "Configuration Reload Interval",
          "description" : "Interval in minutes to fetch agent configuration from AM. (property name:
com.sun.identity.agents.config.polling.interval) <br>Required Agent Restart",
          "propertyOrder" : 25900,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "notificationsEnabled" : {
          "title" : "Enable Notifications",
          "description" : "The notifications help in maintaining agent's sso, policy and configuration
caches. (property name: com.sun.identity.agents.config.notification.enable) <br>Required Agent
Restart",
```

```
          "propertyOrder" : 25600,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "webSocketConnectionIntervalInMinutes" : {
          "title" : "Web Socket Connection Interval",
          "description" : "Interval in minutes by which agents reopen their web socket
connection to ensure a fair distribution of connections across AM servers. (property:
org.forgerock.agents.balance.websocket.interval.minutes).",
          "propertyOrder" : 25400,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "auditLogLocation" : {
          "title" : "Audit Log Location",
          "description" : "Specifies where audit messages should be logged. (property name:
com.sun.identity.agents.config.log.disposition)",
          "propertyOrder" : 26800,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "auditAccessType" : {
          "title" : "Audit Access Types",
          "description" : "Types of messages to log based on user URL access attempts. (property name:
com.sun.identity.agents.config.audit.accesstype)",
          "propertyOrder" : 26700,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "ssoOnlyMode" : {
          "title" : "SSO Only Mode",
          "description" : "Agent will just enforce authentication (SSO), but no authorization for
policies. (property name: com.sun.identity.agents.config.sso.only)",
          "propertyOrder" : 26200,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "resetIdleTime" : {
          "title" : "Reset Idle Timeout",
          "description" : "If the agent is configured in SSO-only mode, the session may unexpectedly
expire in AM due to idle timeout before the user has finished accessing the application. <br>Set
this property to true to refresh the timeout when the user performs an action. <br>When set to
true, the agent makes an additional call to AM, this may cause a performance impact. Configure this
property only if: <br>   The agent is configured in SSO-only mode. <br>   User's sessions are timing
out in AM because they are unexpectedly reaching the maximum idle timeout value. <br>(property:
com.forgerock.agents.call.session.refresh)",
          "propertyOrder" : 26250,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "cdssoRootUrl" : {
          "title" : "Agent Root URL for CDSSO",
```

```
          "description" : "The agent root URL for CDSSO. The valid value is in the following format:
<br>protocol://hostname:port/<br> The protocol represents the protocol used, such as http or https.
The hostname represents the host name of the machine on which the agent resides. The port represents
the port number on which the agent is installed. The slash following the port number is required.",
          "propertyOrder" : 26100,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        }
      }
    },
    "amServicesWebAgent" : {
      "type" : "object",
      "title" : "AM Services",
      "propertyOrder" : 3,
      "properties" : {
        "fetchPoliciesFromRootResource" : {
          "title" : "Fetch Policies from Root Resource",
          "description" : "Agent caches policy decision of the resource and all resources from the
root of the resource down. (property name: com.sun.identity.agents.config.fetch.from.root.resource)
<br>Required Agent Restart",
          "propertyOrder" : 31000,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "customLoginMode" : {
          "title" : "Custom Login Mode",
          "description" : "Specifies whether the agent should use the default or the custom login
mode when redirecting unauthenticated users.<br>Possible values are: <br>0. Disabled. Default login
redirection mode enabled <br>  1. Custom login mode enabled based on converts the SSO token into an
ID token <br>  2. Legacy Custom login mode. Can be used in specific migration cases from agent 4
<br>(property: org.forgerock.openam.agents.config.allow.custom.login)",
          "propertyOrder" : 29890,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "publicAmUrl" : {
          "title" : "Public AM URL",
          "description" : "Overrides the agent's behavior of finding a suitable AM server and
specifies the public URL of the AM to redirect to. <br> Use this property if: <br>  - Your
environment uses custom login pages (OIDC-compliant and non-OIDC-compliant flows). <br>  - Your
environment's custom login pages are in a network that can only access AM using a proxy, a firewall,
or any other technology that remaps the AM URL to one accessible by the custom login pages. <br>
 -End-users cannot log in due to their cookies being set in the wrong domains. <br>(property:
com.forgerock.agents.public.am.url) ",
          "propertyOrder" : 29950,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "logoutUrlRegex" : {
          "title" : "Logout URL Regular Expression",
          "description" : "Perl-compatible regular expression that matches logout URLs. For
example, to match URLs with protectedA or protectedB in the path and op=logout in the query
```

```
 string, use the following setting: <br>*(/protectedA\\?|/protectedB\\?/).*(\\&op=logout\\&)(.*|$)
  <br>When you use this property, the agent ignores the settings for Logout URL List. (property:
 com.forgerock.agents.agent.logout.url.regex)",
          "propertyOrder" : 30540,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "retrieveClientHostname" : {
          "title" : "Retrieve Client Hostname",
          "description" : "Gets the client's hostname through DNS reverse lookup for use in policy
 evaluation. (property name: com.sun.identity.agents.config.get.client.host.name)",
          "propertyOrder" : 31100,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "applicationLogoutUrls" : {
          "title" : "Logout URL List",
          "description" : "List of application logout URLs. User gets logged out from AM session
 when these urls accessed. (property name: com.sun.identity.agents.config.agent.logout.url). If
 this property is used, user should specify a value for the below Logout Redirect URL property. <br>
 Example: <br> http://myagent.mydomain.com/logout.html",
          "propertyOrder" : 30300,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "enableLogoutRegex" : {
          "title" : "Enable Regex for Logout URL List",
          "description" : "This property allows regular expressions in \"Logout URL List\" (property:
 org.forgerock.agents.config.logout.regex.enable)",
          "propertyOrder" : 30530,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "regexConditionalLoginUrl" : {
          "title" : "Regular Expression Conditional Login URL",
          "description" : "Conditionally redirect users based on the incoming request URL. If the
 incoming request URL matches a regular expression, the web agent redirects the request to a specific
 URL. That specific URL can be an AM instance, site, or a different website. Specifies the redirection
 URL and its parameters. This property needs to configure \"Regular Expression Conditional Login
 Pattern\" <br>Example: <br>  org.forgerock.agents.config.conditional.login.pattern[0] = .*shop <br>
  org.forgerock.agents.config.conditional.login.url[0] = http://openam.example.com/openam/oauth2/
authorize?realm=sales <br>(property: org.forgerock.agents.config.conditional.login.url)",
          "propertyOrder" : 30100,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "userIdParameter" : {
          "title" : "User ID Parameter",
```

```
          "description" : "Agent sets value of User Id to REMOTE_USER server variable. (property name:
 com.sun.identity.agents.config.userid.param)",
          "propertyOrder" : 30800,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "regexConditionalLoginPattern" : {
          "title" : "Regular Expression Conditional Login Pattern",
          "description" : "Conditionally redirect users based on the incoming request
 URL. If the incoming request URL matches a regular expression, the web agent redirects
 the request to a specific URL. That specific URL can be an AM instance, site, or
 a different website. Specifies the regular expression that the domain name must
 match. This property needs to configure \"Regular Expression Conditional Login URL\"
 <br>Example: <br>  org.forgerock.agents.config.conditional.login.pattern[0] = .*shop <br>
 org.forgerock.agents.config.conditional.login.url[0] = http://openam.example.com/openam/oauth2/
authorize?realm=sales <br>(property: org.forgerock.agents.config.conditional.login.pattern)",
          "propertyOrder" : 30050,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "logoutResetCookies" : {
          "title" : "Logout Cookies List for Reset",
          "description" : "Any cookies to be reset upon logout in the same format as cookie reset
 list. (property name: com.sun.identity.agents.config.logout.cookie.reset) <br> Cookie1 <br>
 Cookie2=value;Domain=subdomain.domain.com",
          "propertyOrder" : 30400,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "policyClockSkew" : {
          "title" : "Policy Clock Skew",
          "description" : "Time in seconds used adjust time difference between Agent
 machine and AM. Clock skew in seconds = AgentTime - AMServerTime. (property name:
 com.sun.identity.agents.config.policy.clock.skew) <br>Required Agent Restart",
          "propertyOrder" : 31200,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "conditionalLoginUrl" : {
          "title" : "AM Conditional Login URL",
          "description" : "Conditionally redirect users based on the incoming request URL. If
 the incoming request URL matches a specified domain name, the web agent redirects the request
 to a specific URL. That specific URL can be an AM instance, site, or a different website.
 <br>Example: <br>  example.com|https://openam.example.com/openam/oauth2/authorize <br>
 myapp.domain.com|https://openam2.example.com/openam/oauth2/authorize?realm=sales (property:
 com.forgerock.agents.conditional.login.url)",
          "propertyOrder" : 30000,
          "required" : false,
          "items" : {
```

```
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "policyCachePollingInterval" : {
          "title" : "Policy Cache Polling Period",
          "description" : "Polling interval in minutes to refresh agent's policy cache. (property
name: com.sun.identity.agents.config.policy.cache.polling.interval) <br>Required Agent Restart",
          "propertyOrder" : 30600,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "amLoginUrl" : {
          "title" : "AM Login URL",
          "description" : "AM login page URL. (property name:
com.sun.identity.agents.config.login.url)  <br> Example: <br> http://host:port/am/UI/Login",
          "propertyOrder" : 29900,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "invalidateLogoutSession" : {
          "title" : "Invalidate Logout Session",
          "description" : "Specifies whether the agent must invalidate the
user session in AM when redirecting to the logout URL specified either by the
Logout URL list (com.sun.identity.agents.config.agent.logout.url) or the AM
logout URL (com.sun.identity.agents.config.logout.url) properties. (property:
org.forgerock.agents.config.logout.session.invalidate)",
          "propertyOrder" : 30520,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "policyEvaluationRealm" : {
          "title" : "Policy Evaluation Realm",
          "description" : "Which realm to start evaluating from. (property name:
org.forgerock.openam.agents.config.policy.evaluation.realm)",
          "propertyOrder" : 31300,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "userIdParameterType" : {
          "title" : "User ID Parameter Type",
          "description" : "User ID can be fetched from either SESSION and LDAP attributes. (property
name: com.sun.identity.agents.config.userid.param.type)",
          "propertyOrder" : 30900,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "ssoCachePollingInterval" : {
          "title" : "SSO Cache Polling Period",
```

```
          "description" : "Polling interval in minutes to refresh agent's sso cache. (property name:
com.sun.identity.agents.config.sso.cache.polling.interval) <br>Required Agent Restart",
          "propertyOrder" : 30700,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "logoutRedirectUrl" : {
          "title" : "Logout Redirect URL",
          "description" : "User gets redirected to this url after logout. (property name:
com.sun.identity.agents.config.logout.redirect.url). This property should be specified along with the
above Logout URL List.",
          "propertyOrder" : 30500,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "amLogoutUrl" : {
          "title" : "AM Logout URL",
          "description" : "AM logout page URL. (property name:
com.sun.identity.agents.config.logout.url)  <br> Example: <br> http://host:port/am/UI/Logout",
          "propertyOrder" : 30200,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "logoutRedirectDisabled" : {
          "title" : "Disabled Logout Redirection",
          "description" : "When disabled, instead of redirecting the user-agent, the web agent
performs session logout in the background and then continues processing access to the current URL.
(property: com.forgerock.agents.config.logout.redirect.disable)",
          "propertyOrder" : 30510,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "policyEvaluationApplication" : {
          "title" : "Policy Set",
          "description" : "Which application contains the policies to evaluate with. (property name:
org.forgerock.openam.agents.config.policy.evaluation.application)",
          "propertyOrder" : 31400,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "ssoWebAgentConfig" : {
      "type" : "object",
      "title" : "SSO",
      "propertyOrder" : 2,
      "properties" : {
        "cookieName" : {
          "title" : "Cookie Name",
          "description" : "Name of the SSO Token cookie used between the AM server and the Agent.
(property name: com.sun.identity.agents.config.cookie.name)<br>Required Agent Restart",
```

```
          "propertyOrder" : 29100,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "persistentJwtCookie" : {
          "title" : "Persistent JWT Cookie",
          "description" : "Enable persistence for JWT cookie. If true JWT cookie will not be set as
Session Cookie. (property: org.forgerock.agents.config.cdsso.persistent.cookie.enable)",
          "propertyOrder" : 29270,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "cdssoRedirectUri" : {
          "title" : "CDSSO Redirect URI",
          "description" : "An intermediate URI that is used by the Agent for processing CDSSO
requests. (property name: org.forgerock.agents.authn.redirect.uri) ",
          "propertyOrder" : 29300,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "cookieResetOnRedirect" : {
          "title" : "Session Cookie Reset on Authentication Redirect",
          "description" : "When set to true. the agent will not reset the session cookie on an
authentication redirect if there is a policy advice present.By default, the agent resets the session
cookie in all configured domains on every authentication redirect when a policy advice is present.
(property: org.forgerock.agents.config.cdsso.advice.cleanup.disable)",
          "propertyOrder" : 29400,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "cookieResetEnabled" : {
          "title" : "Cookie Reset",
          "description" : "Agent resets cookies in the response before redirecting to authentication.
(property name: com.sun.identity.agents.config.cookie.reset.enable)",
          "propertyOrder" : 29700,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "secureCookies" : {
          "title" : "Cookie Security",
          "description" : "Agent sends secure cookies if communication is secure. (property name:
com.sun.identity.agents.config.cookie.secure) <br>Required Agent Restart",
          "propertyOrder" : 29200,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "acceptSsoToken" : {
          "title" : "Accept SSO Token",
          "description" : "Specifies whether the agent should accept SSO tokens as session
cookies alongside with ID tokens. Possible values: <br>- false. The agent does not accept SSO
Tokens <br>- true. The agent accepts both SSO tokens and ID tokens as session tokens during
the login flow, and afterwards. SSO tokens are not converted to ID tokens <br>Set this property
```

```
to \"true\" only for specific migration cases (see documentation for more info) <br>(property:
com.forgerock.agents.accept.sso.token) (Agent 5.7+ only)",
          "propertyOrder" : 29850,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "httpOnly" : {
          "title" : "HTTP Only Mode",
          "description" : "Agents with this property set to true mark cookies as HTTPOnly
to prevent scripts and third-party programs from accessing the cookies. (property:
com.sun.identity.cookie.httponly)",
          "propertyOrder" : 29250,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "multivaluePreAuthnCookie" : {
          "title" : "Multivalue for Pre-Authn Cookie",
          "description" : "With this set, the agent will use a legacy mode to create cookies that are
used to track unauthenticated requests that have been redirected to login. This mode should only be
used for backward compatibility, where the pre-5.7 way of tracking redirected requests is required,
perhaps because the cookie names are referenced in proxy configuration. This property need not be set
in any other situation. (property: org.forgerock.openam.agents.config.multivalue.pre.authn.cookies)",
          "propertyOrder" : 29280,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "cookieResetList" : {
          "title" : "Cookies Reset Name List",
          "description" : "List of cookies in the format: name[=value][;Domain=value].
(property name: com.sun.identity.agents.config.cookie.reset) <br> Examples: <br> Cookie1 <br>
Cookie2=value;Domain=subdomain.domain.com",
          "propertyOrder" : 29800,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "sameSite" : {
          "title" : "SameSite Cookie Attribute",
          "description" : "If set, agent will add SameSite attribute to all cookies created by
agent with value which is provided in this property. <br>Example: Strict, Lax, None (property:
com.forgerock.agents.cdsso.cookie.samesite)",
          "propertyOrder" : 29260,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "cdssoCookieDomain" : {
          "title" : "Cookies Domain List",
          "description" : "List of domains in which cookies have to be set in CDSSO. (property name:
com.sun.identity.agents.config.cdsso.cookie.domain) <br> Example: <br> .example.com",
          "propertyOrder" : 29600,
          "required" : false,
          "items" : {
```

```
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        }
      }
    },
    "advancedWebAgentConfig" : {
      "type" : "object",
      "title" : "Advanced",
      "propertyOrder" : 5,
      "properties" : {
        "pdpStickySessionMode" : {
          "title" : "POST Data Sticky Load Balancing Mode",
          "description" : "Specifies whether to create a cookie, or to append a
query string to the URL to assist with sticky load balancing. Possible values
are: <br>COOKIE. The web agent creates a cookie with the value specified
in the com.sun.identity.agents.config.postdata.preserve.stickysession.value
property. <br>URL. The web agent appends the value specified in the
com.sun.identity.agents.config.postdata.preserve.stickysession.value to the URL query string. <br>
(property: com.sun.identity.agents.config.postdata.preserve.stickysession.mode)",
          "propertyOrder" : 33700,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "pdpStickySessionValue" : {
          "title" : "POST Data Sticky Load Balancing Value",
          "description" : "Specifies a key-value pair separated by the = character that the web
agent creates when evaluating the \"POST Data Sticky Load Balancing Mode\". For example, a setting
of lb=myserver either sets an lb cookie with myserver value, or adds lb=myserver to the URL query
string. When configuring POST data preservation with cookies, set the cookie name in the cookie
pair to the same value configured in the \"POST Data Sticky Load Balancing Cookie Name\". (property:
com.sun.identity.agents.config.postdata.preserve.stickysession.value)",
          "propertyOrder" : 33710,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "logonAndImpersonation" : {
          "title" : "Logon and Impersonation",
          "description" : "Set to true if agent should do Windows Logon and User Impersonation.
(property name: com.sun.identity.agents.config.iis.logonuser)",
          "propertyOrder" : 34500,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "clientHostnameHeader" : {
          "title" : "Client Hostname Header",
          "description" : "HTTP header name that holds the Hostname of the client. (property name:
org.forgerock.agents.http.header.containing.remote.hostname) ",
          "propertyOrder" : 32900,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "fragmentRedirectEnabled" : {
          "title" : "Fragment Redirect Enabled",
```

```
          "description" : "Enable to save the browser's URL fragment during authentication.
<br>(property: org.forgerock.agents.config.fragment.redirect.enable) (Agent 5.7+ only)",
          "propertyOrder" : 33400,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "postDataPreservation" : {
          "title" : "POST Data Preservation",
          "description" : "Enables POST data preservation. (property name:
com.sun.identity.agents.config.postdata.preserve.enable) <br> Note that this feature is not supported
in all the web agents. Please refer individual agents documentation for more details.",
          "propertyOrder" : 33500,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "overrideRequestPort" : {
          "title" : "Override Request URL Port",
          "description" : "Set to true if the agent is sitting behind a ssl/tls
off-loader, load balancer, or proxy to override the port with the value from
the property com.sun.identity.agents.config.agenturi.prefix. (property name:
com.sun.identity.agents.config.override.port)",
          "propertyOrder" : 33300,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "pdpJavascriptRepost" : {
          "title" : "Show Password in HTTP Header",
          "description" : "Set to true if encrypted password should be set in HTTP header
AUTH_PASSWORD. (property name: com.sun.identity.agents.config.iis.password.header)",
          "propertyOrder" : 33730,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "clientIpHeader" : {
          "title" : "Client IP Address Header",
          "description" : "HTTP header name that holds the IP address of the client. (property name:
org.forgerock.agents.http.header.containing.ip.address) ",
          "propertyOrder" : 32800,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "postDataCachePeriod" : {
          "title" : "POST Data Entries Cache Period",
          "description" : "POST cache entry lifetime in minutes. (property name:
com.sun.identity.agents.config.postcache.entry.lifetime)",
          "propertyOrder" : 33600,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "replayPasswordKey" : {
          "title" : "Replay Password Key",
          "description" : "DES key for decrypting the basic authentication password in the session.
(property name: com.sun.identity.agents.config.replaypasswd.key)",
```

```
          "propertyOrder" : 33900,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "customProperties" : {
          "title" : "Custom Properties",
          "description" : "Additional properties that allow users to augment the set of
properties supported by agent. (property name: com.sun.identity.agents.config.freeformproperties)
 <br> Examples: <br> customproperty=custom-value1 <br> customlist[0]=customlist-value-0
<br> customlist[1]=customlist-value-1 <br> custommap[key1]=custommap-value-1 <br>
custommap[key2]=custommap-value-2",
          "propertyOrder" : 35100,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "overrideRequestProtocol" : {
          "title" : "Override Request URL Protocol",
          "description" : "Set to true if the agent is sitting behind a ssl/tls
off-loader, load balancer, or proxy to override the protocol with the value from
the property com.sun.identity.agents.config.agenturi.prefix. (property name:
com.sun.identity.agents.config.override.protocol)",
          "propertyOrder" : 33100,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "showPasswordInHeader" : {
          "title" : "Show Password in HTTP Header",
          "description" : "Set to true if encrypted password should be set in HTTP header
AUTH_PASSWORD. (property name: com.sun.identity.agents.config.iis.password.header)",
          "propertyOrder" : 34400,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "pdpStickySessionCookieName" : {
          "title" : "POST Data Sticky Load Balancing Cookie Name",
          "description" : "Specifies the name of a cookie to use for enabling sticky load balancing
when the \"POST Data Sticky Load Balancing Mode\" property is set to COOKIE. Set the cookie name
to the same value configured in the \"POST Data Sticky Load Balancing Value\" property. (property:
com.sun.identity.agents.config.postdata.preserve.lbcookie)",
          "propertyOrder" : 33720,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "overrideRequestHost" : {
          "title" : "Override Request URL Host",
          "description" : "Set to true if the agent is sitting behind a ssl/tls
off-loader, load balancer, or proxy to override the host with the value from
the property com.sun.identity.agents.config.agenturi.prefix. (property name:
com.sun.identity.agents.config.override.host)",
          "propertyOrder" : 33200,
          "required" : false,
```

```
          "type" : "boolean",
          "exampleValue" : ""
        },
        "pdpSkipPostUrl" : {
          "title" : "URLs Ignored by the Agent POST Data Inspector",
          "description" : "Specifies a list of URLs that will not be processed by the web agent
 POST data inspector. This allows other modules on the same server to access the POST data directly.
 <br>The following example uses wildcards to add a file named postreader.jsp in the root of any
 protected website to the list of URLs that will not have their POST data inspected: <br>http*://*:*/
postreader.jsp <br>Any URLs added to this property should also be added to the Not-Enforced URLs <br>
 (property: org.forgerock.agents.config.skip.post.url)",
          "propertyOrder" : 33740,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        }
      }
    },
    "miscWebAgentConfig" : {
      "type" : "object",
      "title" : "Miscellaneous",
      "propertyOrder" : 4,
      "properties" : {
        "addCacheControlHeader" : {
          "title" : "Add Cache-Control Headers",
          "description" : "Set this property to true to enable use of Cache-Control headers
 that prevent proxies from caching resources accessed by unauthenticated users. (property:
 com.forgerock.agents.cache_control_header.enable)",
          "propertyOrder" : 32710,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "urlJsonResponse" : {
          "title" : "URLs to Receive JSON-Formatted Responses",
          "description" : "Returning the responses in JSON format is useful for non-
browser-based, or AJAX applications, that may not want to redirect users to the AM user
 interface for authentication. <br>Example: org.forgerock.agents.config.json.url[0]=http*://
*.example.com:*/api/* <br>org.forgerock.agents.config.json.response.code=202 <br>(property:
 org.forgerock.agents.config.json.url)",
          "propertyOrder" : 32730,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "anonymousUserId" : {
          "title" : "Anonymous User Default Value",
          "description" : "User id of unauthenticated users. (property name:
 com.sun.identity.agents.config.anonymous.user.id)",
          "propertyOrder" : 32700,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
```

```
      },
      "statusCodeJsonResponse" : {
        "title" : "HTTP Return Code for JSON-Formatted Responses",
        "description" : "Specifies an HTTP response code to return when a JSON-formatted error is
triggered. (property: org.forgerock.agents.config.json.response.code)",
        "propertyOrder" : 32760,
        "required" : false,
        "type" : "integer",
        "exampleValue" : ""
      },
      "encodeUrlSpecialCharacters" : {
        "title" : "Encode URL's Special Characters",
        "description" : "Encodes the url which has special characters before doing policy
evaluation. (property name: com.sun.identity.agents.config.encode.url.special.chars.enable)",
        "propertyOrder" : 32100,
        "required" : false,
        "type" : "boolean",
        "exampleValue" : ""
      },
      "mineEncodeHeader" : {
        "title" : "MIME-Encode HTTP Header Values",
        "description" : "Specifies whether the agent must MIME-encode HTTP header values, and
when to do it. Possible values are: <br>  0. The agent MIME-encodes the value of HTTP headers
if said value is a multi-byte Unicode string. <br>  1. The agent MIME-encodes the value of every
HTTP header. <br>  2. The agent does not MIME-encode the value of any HTTP header. <br> (property:
com.forgerock.agents.header.mime.encode)",
        "propertyOrder" : 32720,
        "required" : false,
        "type" : "integer",
        "exampleValue" : ""
      },
      "compositeAdviceEncode" : {
        "title" : "Composite Advice Encode",
        "description" : "This property is used to specify whether AM composite advices
should be based64url encoded before sending to custom login endpoints. (property:
com.forgerock.agents.advice.b64.url.encode)",
        "propertyOrder" : 32300,
        "required" : false,
        "type" : "boolean",
        "exampleValue" : ""
      },
      "compositeAdviceRedirect" : {
        "title" : "Composite Advice Handling",
        "description" : "When set to true, the agent sends composite advice in
the query (GET request) instead of sending it through a POST request. (property:
com.sun.am.use_redirect_for_advice)",
        "propertyOrder" : 32200,
        "required" : false,
        "type" : "boolean",
        "exampleValue" : ""
      },
      "ignorePathInfo" : {
        "title" : "Ignore Path Info in Request URL",
        "description" : "The path info will be stripped from the request URL while doing Not
Enforced List check and url policy evaluation if the value is set to true. (property name:
com.sun.identity.agents.config.ignore.path.info)",
        "propertyOrder" : 32400,
        "required" : false,
        "type" : "boolean",
```

```
          "exampleValue" : ""
        },
        "gotoParameterName" : {
          "title" : "Goto Parameter Name",
          "description" : "This is the name of the HTTP query \"goto\" parameter. It is not
recommended to change it. (property name: com.sun.identity.agents.config.redirect.param) ",
          "propertyOrder" : 32600,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "invertUrlJsonResponse" : {
          "title" : "Invert Properties That Receive JSON-Formatted Responses",
          "description" : "Set to true to invert the meaning of both the
org.forgerock.agents.config.json.url and org.forgerock.agents.config.json.header properties.
When inverted the specified values in those two properties will not trigger JSON-formatted
responses. Any non-specified value will trigger JSON-formatted responses, instead. (property:
org.forgerock.agents.config.json.url.invert)",
          "propertyOrder" : 32750,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "invalidUrlRegex" : {
          "title" : "Invalid URL Regular Expression",
          "description" : "Specifies a Perl-compatible regular expression to parse valid request
URLs. The web agent rejects requests to invalid URLs with HTTP 403 Forbidden status without
further processing. <br>Example, to filter out URLs containing a list of characters and words
such as ./ /. / . %00-%1f, %7f-%ff, %25, %2B, %2C, %7E, .info, configure the following regular
expression: <br>^(\\?!.\\/|\\/.|.|.info|%2B|%00-%1f|%7f-%ff|%25|%2C|%7E).*$ <br>(property:
com.forgerock.agents.agent.invalid.url.regex)",
          "propertyOrder" : 32500,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "profileAttributesCookiePrefix" : {
          "title" : "Profile Attributes Cookie Prefix",
          "description" : "Sets cookie prefix in the attributes headers. (property name:
com.sun.identity.agents.config.profile.attribute.cookie.prefix)",
          "propertyOrder" : 31800,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "headerJsonResponse" : {
          "title" : "Headers and Values to Receive JSON-Formatted Responses",
          "description" : "Specify HTTP headers and associated values
that trigger JSON-formatted errors to be returned. <br>Example:
<br>org.forgerock.agents.config.json.header[enableJsonResponse]=true
<br>org.forgerock.agents.config.json.response.code=202 <br>(property:
org.forgerock.agents.config.json.header[Header]=Value)",
          "propertyOrder" : 32740,
          "required" : false,
          "patternProperties" : {
            ".*" : {
              "type" : "string"
            }
          },
```

```
          "type" : "object",
          "exampleValue" : ""
        },
        "encodeSpecialCharsInCookies" : {
          "title" : "Encode special chars in Cookies",
          "description" : "Encode special chars in cookie by URL encoding. Useful when profile,
 session and response attributes contain special chars and attributes fetch mode is set to
 HTTP_COOKIE. (property name: com.sun.identity.agents.config.encode.cookie.special.chars.enable)  ",
          "propertyOrder" : 31700,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "caseInsensitiveUrlComparison" : {
          "title" : "URL Comparison Case Sensitivity Check",
          "description" : "Enforces case insensitivity in both policy and not enforced url evaluation.
 (property name: com.sun.identity.agents.config.url.comparison.case.ignore)",
          "propertyOrder" : 32000,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "anonymousUserEnabled" : {
          "title" : "Anonymous User",
          "description" : "Enable/Disable REMOTE_USER processing for anonymous users. (property name:
 com.sun.identity.agents.config.anonymous.user.enable)",
          "propertyOrder" : 31600,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "profileAttributesCookieMaxAge" : {
          "title" : "Profile Attributes Cookie Maxage",
          "description" : "Maxage of attributes cookie headers. (property name:
 com.sun.identity.agents.config.profile.attribute.cookie.maxage)",
          "propertyOrder" : 31900,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        }
      }
    }
  }
}
```

delete

Usage:

```
am> delete WebAgentGroups --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action WebAgentGroups --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action WebAgentGroups --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action WebAgentGroups --realm Realm --actionName nextdescendents
```

query

Querying the agent groups of a specific type

Usage:

```
am> query WebAgentGroups --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read WebAgentGroups --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update WebAgentGroups --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "applicationWebAgentConfig" : {
      "type" : "object",
      "title" : "Application",
      "propertyOrder" : 1,
      "properties" : {
        "continuousSecurityCookies" : {
          "title" : "Continuous Security Cookies",
          "description" : "The name of the cookies to be sent as part of the payload during policy
 evaluation, which can be accessed via the 'environment' variable in a policy script. The 'key' is
 the name of the cookie to be sent, and the 'value' is the name which it will appear as in the policy
 evaluation script. It is possible to map multiple cookies to the same name (they will simply appear
 as an array in the evaluation script). If the cookie doesn't exist, then the empty string will be
 sent.",
          "propertyOrder" : 28900,
          "required" : false,
          "patternProperties" : {
            ".*" : {
              "type" : "string"
            }
          },
          "type" : "object",
          "exampleValue" : ""
        },
        "profileAttributeFetchMode" : {
          "title" : "Profile Attribute Fetch Mode",
          "description" : "(property name:
 com.sun.identity.agents.config.profile.attribute.fetch.mode)",
          "propertyOrder" : 28200,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "notEnforcedIpsRegex" : {
          "title" : "Regular Expressions for Not-Enforced IPs",
          "description" : "Enable use of Perl-compatible regular expressions in Not-Enforced URL from
 IP settings. (property: org.forgerock.agents.config.notenforced.ext.regex.enable)",
          "propertyOrder" : 28150,
          "required" : false,
          "type" : "boolean",
```

```
          "exampleValue" : ""
        },
        "sessionAttributeFetchMode" : {
          "title" : "Session Attribute Fetch Mode",
          "description" : "(property name:
 com.sun.identity.agents.config.session.attribute.fetch.mode)",
          "propertyOrder" : 28600,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "continuousSecurityHeaders" : {
          "title" : "Continuous Security Headers",
          "description" : "The name of the headers in the user's original request, that will be sent
 as part of the payload during policy evaluation, which can then be accessed via the 'environment'
 variable in a policy script. The 'key' is the name of the header to be sent, and the 'value' is the
 name which it will appear as in the policy evaluation script.It is possible to map multiple headers
 to the same name (they will simply appear as an array in the evaluation script). If the header
 doesn't exist, then the empty string will be sent.",
          "propertyOrder" : 29000,
          "required" : false,
          "patternProperties" : {
            ".*" : {
              "type" : "string"
            }
          },
          "type" : "object",
          "exampleValue" : ""
        },
        "notEnforcedIpsList" : {
          "title" : "Not-Enforced URL from IP Processing List",
          "description" : "Specifies a list of client IP addresses that do not require authentication
 when requesting the indicated URLs. <br>The supported format requires a list of IP addresses
 separated by spaces, the horizontal bar (|) character, and a list of URLs separated by spaces.
 <br>For example: <br>  10.1.2.1 192.168.0.2|/public/* <br>In the preceding example, the IP addresses
 10.1.2.1 and  192.168.0.2 can access any resource inside /public without authenticating. (property:
 org.forgerock.agents.config.notenforced.ipurl)",
          "propertyOrder" : 28050,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "notEnforcedUrlsRegex" : {
          "title" : "Regular Expressions for Not-Enforced URLs",
          "description" : "When true, enables use of Perl-compatible regular expressions in Not-
enforced URL settings. (property: com.forgerock.agents.notenforced.url.regex.enable)",
          "propertyOrder" : 27850,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "sessionAttributeMap" : {
          "title" : "Session Attribute Map",
          "description" : "Maps the session attributes to be populated
 under specific names for the currently authenticated user. (property name:
 com.sun.identity.agents.config.session.attribute.mapping)   <br> Example: <br>  To populate the value
```

```
 of session attribute UserToken under name CUSTOM-userid: enter UserToken in Map Key field, and enter
 CUSTOM-userid in Corresponding Map Value field.",
          "propertyOrder" : 28700,
          "required" : false,
          "patternProperties" : {
            ".*" : {
              "type" : "string"
            }
          },
          "type" : "object",
          "exampleValue" : ""
        },
        "responseAttributeMap" : {
          "title" : "Response Attribute Map",
          "description" : "Maps the policy response attributes to be populated
 under specific names for the currently authenticated user. (property name:
 com.sun.identity.agents.config.response.attribute.mapping)  <br> Example: <br> To populate the value
 of response attribute uid under name CUSTOM-USER-NAME: enter uid in Map Key field, and enter CUSTOM-
USER-NAME in Corresponding Map Value field.",
          "propertyOrder" : 28500,
          "required" : false,
          "patternProperties" : {
            ".*" : {
              "type" : "string"
            }
          },
          "type" : "object",
          "exampleValue" : ""
        },
        "profileAttributeMap" : {
          "title" : "Profile Attribute Map",
          "description" : "Maps the profile attributes to be populated
 under specific names for the currently authenticated user. (property name:
 com.sun.identity.agents.config.profile.attribute.mapping)  <br> Example: <br> To populate the value
 of profile attribute cn under name CUSTOM-Common-Name: enter cn in Map Key field, and enter CUSTOM-
Common-Name in Corresponding Map Value field. <br> To populate the value of profile attribute mail
 under name CUSTOM-Email: enter mail in Map Key field, and enter CUSTOM-Email in Corresponding Map
 Value field.",
          "propertyOrder" : 28300,
          "required" : false,
          "patternProperties" : {
            ".*" : {
              "type" : "string"
            }
          },
          "type" : "object",
          "exampleValue" : ""
        },
        "fetchAttributesForNotEnforcedUrls" : {
          "title" : "Fetch Attributes for Not Enforced URLs",
          "description" : "Agent fetches profile attributes for not enforced urls by doing policy
 evaluation. (property name: com.sun.identity.agents.config.notenforced.url.attributes.enable)",
          "propertyOrder" : 27900,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "attributeMultiValueSeparator" : {
          "title" : "Attribute Multi Value Separator",
```

```
          "description" : "Specifies separator for multiple values. Applies to all
 types of attributes i.e. profile, session and response attributes. (property name:
 com.sun.identity.agents.config.attribute.multi.value.separator)",
          "propertyOrder" : 28800,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "invertNotEnforcedUrls" : {
          "title" : "Invert Not Enforced URLs",
          "description" : "Only not enforced list of urls will be enforced. (property name:
 com.sun.identity.agents.config.notenforced.url.invert)",
          "propertyOrder" : 27800,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "ignorePathInfoForNotEnforcedUrls" : {
          "title" : "Ignore Path Info for Not Enforced URLs",
          "description" : "Indicate whether the path info and query should be
 stripped from the request URL before being compared with the URLs of the not
 enforced list when those URLs have a wildcard '*' character.  (property name:
 com.sun.identity.agents.config.ignore.path.info.for.not.enforced.list)  ",
          "propertyOrder" : 27600,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "responseAttributeFetchMode" : {
          "title" : "Response Attribute Fetch Mode",
          "description" : "(property name:
 com.sun.identity.agents.config.response.attribute.fetch.mode)",
          "propertyOrder" : 28400,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "notEnforcedIps" : {
          "title" : "Not Enforced Client IP List",
          "description" : "No authentication and authorization are required for the requests coming
 from these client IP addresses. (property name: com.sun.identity.agents.config.notenforced.ip) <br>
 Examples: <br> 192.18.145.* <br> 192.18.146.123",
          "propertyOrder" : 28000,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "notEnforcedUrls" : {
          "title" : "Not Enforced URLs",
          "description" : "List of urls for which no authentication required. (property name:
 com.sun.identity.agents.config.notenforced.url) <br> Example: <br> http://myagent.mydomain.com/
*.gif",
          "propertyOrder" : 27700,
          "required" : false,
          "items" : {
            "type" : "string"
```

```
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "clientIpValidation" : {
          "title" : "Client IP Validation",
          "description" : "This validates if the subsequent browser requests come from
the same ip address that the SSO token is initially issued against. (property name:
com.sun.identity.agents.config.client.ip.validation.enable)",
          "propertyOrder" : 28100,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        }
      }
    },
    "globalWebAgentConfig" : {
      "type" : "object",
      "title" : "Global",
      "propertyOrder" : 0,
      "properties" : {
        "agentConfigChangeNotificationsEnabled" : {
          "title" : "Agent Configuration Change Notification",
          "description" : "Enable agent to receive notification messages
(via websockets) from AM server for configuration changes. (property name:
org.forgerock.agents.config.change.notifications.enabled) ",
          "propertyOrder" : 25300,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "status" : {
          "title" : "Status",
          "description" : "Status of the agent configuration.",
          "propertyOrder" : 25100,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "jwtName" : {
          "title" : "JWT Cookie Name",
          "description" : "The name used by the agent to set the OIDC JWT on the user's browser.
(property: org.forgerock.agents.jwt.cookie.name)",
          "propertyOrder" : 25500,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "jwtAuditWhitelist" : {
          "title" : "Agent Profile ID Whitelist",
          "description" : "Specifies a comma-separated list of profile IDs that the agent will
consider as valid values for the aud claim. This claim is represented in the JWT containing
the end user's session. <br>Example: <br>agentprofile1,agentprofile2,.... <br>When several
agents configured with different agent profiles protect the same application, set this property
to a list of the agent profiles that are protecting the same application. <br>(property:
com.forgerock.agents.jwt.aud.whitelist)",
          "propertyOrder" : 25520,
          "required" : false,
          "type" : "string",
```

```
        "exampleValue" : ""
      },
      "fqdnCheck" : {
        "title" : "FQDN Check",
        "description" : "Enables checking of fqdn default value and fqdn map values. (property name:
com.sun.identity.agents.config.fqdn.check.enable)",
        "propertyOrder" : 27300,
        "required" : false,
        "type" : "boolean",
        "exampleValue" : ""
      },
      "fqdnDefault" : {
        "title" : "FQDN Default",
        "description" : "Fully qualified hostname that the users should use in order to access
resources. (property name: com.sun.identity.agents.config.fqdn.default)",
        "propertyOrder" : 27400,
        "required" : false,
        "type" : "string",
        "exampleValue" : ""
      },
      "accessDeniedUrl" : {
        "title" : "Resources Access Denied URL",
        "description" : "The URL of the customized access denied page. (property name:
com.sun.identity.agents.config.access.denied.url)",
        "propertyOrder" : 26300,
        "required" : false,
        "type" : "string",
        "exampleValue" : ""
      },
      "agentUriPrefix" : {
        "title" : "Agent Deployment URI Prefix",
        "description" : "(property name: com.sun.identity.agents.config.agenturi.prefix)",
        "propertyOrder" : 25800,
        "required" : false,
        "type" : "string",
        "exampleValue" : ""
      },
      "disableJwtAudit" : {
        "title" : "Disable validation of the audience claim",
        "description" : "Specifies whether the agent should validate the audience claim matches the
agent profile ID represented in the JWT containing the end user's session. <br>Possible values are:
<br>  false = The agent validates audience claim. <br>  true = The agent does not validate audience
claim.<br> (property: com.forgerock.agents.jwt.aud.disable)",
        "propertyOrder" : 25510,
        "required" : false,
        "type" : "boolean",
        "exampleValue" : ""
      },
      "agentDebugLevel" : {
        "title" : "Agent Debug Level",
        "description" : "Agent debug level. (property name:
com.sun.identity.agents.config.debug.level)",
        "propertyOrder" : 26400,
        "required" : false,
        "type" : "string",
        "exampleValue" : ""
      },
      "fqdnMapping" : {
        "title" : "FQDN Virtual Host Map",
```

```
          "description" : "Maps virtual, invalid, or partial hostnames, and IP addresses to the FQDN
to access protected resources. (property name: com.sun.identity.agents.config.fqdn.mapping) <br>
Examples: <br>  To map the partial hostname myserver to myserver.mydomain.com: enter myserver in the
Map Key field and myserver.mydomain.com in the Corresponding Map Value field. To map a virtual server
rst.hostname.com that points to the actual server abc.hostname.com: enter valid1 in the Map Key field
and rst.hostname.com in the Corresponding Map Value field.",
          "propertyOrder" : 27500,
          "required" : false,
          "patternProperties" : {
            ".*" : {
              "type" : "string"
            }
          },
          "type" : "object",
          "exampleValue" : ""
        },
        "configurationPollingInterval" : {
          "title" : "Configuration Reload Interval",
          "description" : "Interval in minutes to fetch agent configuration from AM. (property name:
com.sun.identity.agents.config.polling.interval) <br>Required Agent Restart",
          "propertyOrder" : 25900,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "notificationsEnabled" : {
          "title" : "Enable Notifications",
          "description" : "The notifications help in maintaining agent's sso, policy and configuration
caches. (property name: com.sun.identity.agents.config.notification.enable) <br>Required Agent
Restart",
          "propertyOrder" : 25600,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "webSocketConnectionIntervalInMinutes" : {
          "title" : "Web Socket Connection Interval",
          "description" : "Interval in minutes by which agents reopen their web socket
connection to ensure a fair distribution of connections across AM servers. (property:
org.forgerock.agents.balance.websocket.interval.minutes).",
          "propertyOrder" : 25400,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "auditLogLocation" : {
          "title" : "Audit Log Location",
          "description" : "Specifies where audit messages should be logged. (property name:
com.sun.identity.agents.config.log.disposition)",
          "propertyOrder" : 26800,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "auditAccessType" : {
          "title" : "Audit Access Types",
          "description" : "Types of messages to log based on user URL access attempts. (property name:
com.sun.identity.agents.config.audit.accesstype)",
          "propertyOrder" : 26700,
```

```
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "ssoOnlyMode" : {
          "title" : "SSO Only Mode",
          "description" : "Agent will just enforce authentication (SSO), but no authorization for
policies. (property name: com.sun.identity.agents.config.sso.only)",
          "propertyOrder" : 26200,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "resetIdleTime" : {
          "title" : "Reset Idle Timeout",
          "description" : "If the agent is configured in SSO-only mode, the session may unexpectedly
expire in AM due to idle timeout before the user has finished accessing the application. <br>Set
this property to true to refresh the timeout when the user performs an action. <br>When set to
true, the agent makes an additional call to AM, this may cause a performance impact. Configure this
property only if: <br>   The agent is configured in SSO-only mode. <br>   User's sessions are timing
out in AM because they are unexpectedly reaching the maximum idle timeout value. <br>(property:
com.forgerock.agents.call.session.refresh)",
          "propertyOrder" : 26250,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "cdssoRootUrl" : {
          "title" : "Agent Root URL for CDSSO",
          "description" : "The agent root URL for CDSSO. The valid value is in the following format:
<br>protocol://hostname:port/<br> The protocol represents the protocol used, such as http or https.
The hostname represents the host name of the machine on which the agent resides. The port represents
the port number on which the agent is installed. The slash following the port number is required.",
          "propertyOrder" : 26100,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        }
      }
    },
    "amServicesWebAgent" : {
      "type" : "object",
      "title" : "AM Services",
      "propertyOrder" : 3,
      "properties" : {
        "fetchPoliciesFromRootResource" : {
          "title" : "Fetch Policies from Root Resource",
          "description" : "Agent caches policy decision of the resource and all resources from the
root of the resource down. (property name: com.sun.identity.agents.config.fetch.from.root.resource)
<br>Required Agent Restart",
          "propertyOrder" : 31000,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "customLoginMode" : {
```

```
          "title" : "Custom Login Mode",
          "description" : "Specifies whether the agent should use the default or the custom login
mode when redirecting unauthenticated users.<br>Possible values are: <br>0. Disabled. Default login
redirection mode enabled <br>  1. Custom login mode enabled based on converts the SSO token into an
ID token <br>  2. Legacy Custom login mode. Can be used in specific migration cases from agent 4
<br>(property: org.forgerock.openam.agents.config.allow.custom.login)",
          "propertyOrder" : 29890,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "publicAmUrl" : {
          "title" : "Public AM URL",
          "description" : "Overrides the agent's behavior of finding a suitable AM server and
specifies the public URL of the AM to redirect to. <br> Use this property if: <br>  - Your
environment uses custom login pages (OIDC-compliant and non-OIDC-compliant flows). <br>  - Your
environment's custom login pages are in a network that can only access AM using a proxy, a firewall,
or any other technology that remaps the AM URL to one accessible by the custom login pages. <br>
 -End-users cannot log in due to their cookies being set in the wrong domains. <br>(property:
com.forgerock.agents.public.am.url) ",
          "propertyOrder" : 29950,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "logoutUrlRegex" : {
          "title" : "Logout URL Regular Expression",
          "description" : "Perl-compatible regular expression that matches logout URLs. For
example, to match URLs with protectedA or protectedB in the path and op=logout in the query
string, use the following setting: <br>*(/protectedA\\?|/protectedB\\?/).*(\\&op=logout\\&)(.*|$)
 <br>When you use this property, the agent ignores the settings for Logout URL List. (property:
com.forgerock.agents.agent.logout.url.regex)",
          "propertyOrder" : 30540,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "retrieveClientHostname" : {
          "title" : "Retrieve Client Hostname",
          "description" : "Gets the client's hostname through DNS reverse lookup for use in policy
evaluation. (property name: com.sun.identity.agents.config.get.client.host.name)",
          "propertyOrder" : 31100,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "applicationLogoutUrls" : {
          "title" : "Logout URL List",
          "description" : "List of application logout URLs. User gets logged out from AM session
when these urls accessed. (property name: com.sun.identity.agents.config.agent.logout.url). If
this property is used, user should specify a value for the below Logout Redirect URL property. <br>
Example: <br> http://myagent.mydomain.com/logout.html",
          "propertyOrder" : 30300,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
```

```
        },
        "enableLogoutRegex" : {
          "title" : "Enable Regex for Logout URL List",
          "description" : "This property allows regular expressions in \"Logout URL List\" (property:
 org.forgerock.agents.config.logout.regex.enable)",
          "propertyOrder" : 30530,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "regexConditionalLoginUrl" : {
          "title" : "Regular Expression Conditional Login URL",
          "description" : "Conditionally redirect users based on the incoming request URL. If the
 incoming request URL matches a regular expression, the web agent redirects the request to a specific
 URL. That specific URL can be an AM instance, site, or a different website. Specifies the redirection
 URL and its parameters. This property needs to configure \"Regular Expression Conditional Login
 Pattern\" <br>Example: <br>  org.forgerock.agents.config.conditional.login.pattern[0] = .*shop <br>
  org.forgerock.agents.config.conditional.login.url[0] = http://openam.example.com/openam/oauth2/
authorize?realm=sales <br>(property: org.forgerock.agents.config.conditional.login.url)",
          "propertyOrder" : 30100,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "userIdParameter" : {
          "title" : "User ID Parameter",
          "description" : "Agent sets value of User Id to REMOTE_USER server variable. (property name:
 com.sun.identity.agents.config.userid.param)",
          "propertyOrder" : 30800,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "regexConditionalLoginPattern" : {
          "title" : "Regular Expression Conditional Login Pattern",
          "description" : "Conditionally redirect users based on the incoming request
 URL. If the incoming request URL matches a regular expression, the web agent redirects
 the request to a specific URL. That specific URL can be an AM instance, site, or
 a different website. Specifies the regular expression that the domain name must
 match. This property needs to configure \"Regular Expression Conditional Login URL\"
 <br>Example: <br>  org.forgerock.agents.config.conditional.login.pattern[0] = .*shop <br>
 org.forgerock.agents.config.conditional.login.url[0] = http://openam.example.com/openam/oauth2/
authorize?realm=sales <br>(property: org.forgerock.agents.config.conditional.login.pattern)",
          "propertyOrder" : 30050,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "logoutResetCookies" : {
          "title" : "Logout Cookies List for Reset",
          "description" : "Any cookies to be reset upon logout in the same format as cookie reset
 list. (property name: com.sun.identity.agents.config.logout.cookie.reset) <br> Cookie1 <br>
 Cookie2=value;Domain=subdomain.domain.com",
```

```
          "propertyOrder" : 30400,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "policyClockSkew" : {
          "title" : "Policy Clock Skew",
          "description" : "Time in seconds used adjust time difference between Agent
machine and AM. Clock skew in seconds = AgentTime - AMServerTime. (property name:
com.sun.identity.agents.config.policy.clock.skew) <br>Required Agent Restart",
          "propertyOrder" : 31200,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "conditionalLoginUrl" : {
          "title" : "AM Conditional Login URL",
          "description" : "Conditionally redirect users based on the incoming request URL. If
the incoming request URL matches a specified domain name, the web agent redirects the request
to a specific URL. That specific URL can be an AM instance, site, or a different website.
<br>Example: <br>  example.com|https://openam.example.com/openam/oauth2/authorize <br>
myapp.domain.com|https://openam2.example.com/openam/oauth2/authorize?realm=sales (property:
com.forgerock.agents.conditional.login.url)",
          "propertyOrder" : 30000,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "policyCachePollingInterval" : {
          "title" : "Policy Cache Polling Period",
          "description" : "Polling interval in minutes to refresh agent's policy cache. (property
name: com.sun.identity.agents.config.policy.cache.polling.interval) <br>Required Agent Restart",
          "propertyOrder" : 30600,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "amLoginUrl" : {
          "title" : "AM Login URL",
          "description" : "AM login page URL. (property name:
com.sun.identity.agents.config.login.url)  <br> Example: <br> http://host:port/am/UI/Login",
          "propertyOrder" : 29900,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "invalidateLogoutSession" : {
          "title" : "Invalidate Logout Session",
          "description" : "Specifies whether the agent must invalidate the
user session in AM when redirecting to the logout URL specified either by the
```

```
Logout URL list (com.sun.identity.agents.config.agent.logout.url) or the AM
logout URL (com.sun.identity.agents.config.logout.url) properties. (property:
org.forgerock.agents.config.logout.session.invalidate)",
          "propertyOrder" : 30520,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "policyEvaluationRealm" : {
          "title" : "Policy Evaluation Realm",
          "description" : "Which realm to start evaluating from. (property name:
org.forgerock.openam.agents.config.policy.evaluation.realm)",
          "propertyOrder" : 31300,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "userIdParameterType" : {
          "title" : "User ID Parameter Type",
          "description" : "User ID can be fetched from either SESSION and LDAP attributes. (property
name: com.sun.identity.agents.config.userid.param.type)",
          "propertyOrder" : 30900,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "ssoCachePollingInterval" : {
          "title" : "SSO Cache Polling Period",
          "description" : "Polling interval in minutes to refresh agent's sso cache. (property name:
com.sun.identity.agents.config.sso.cache.polling.interval) <br>Required Agent Restart",
          "propertyOrder" : 30700,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "logoutRedirectUrl" : {
          "title" : "Logout Redirect URL",
          "description" : "User gets redirected to this url after logout. (property name:
com.sun.identity.agents.config.logout.redirect.url). This property should be specified along with the
above Logout URL List.",
          "propertyOrder" : 30500,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "amLogoutUrl" : {
          "title" : "AM Logout URL",
          "description" : "AM logout page URL. (property name:
com.sun.identity.agents.config.logout.url)  <br> Example: <br> http://host:port/am/UI/Logout",
          "propertyOrder" : 30200,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "logoutRedirectDisabled" : {
          "title" : "Disabled Logout Redirection",
```

```
          "description" : "When disabled, instead of redirecting the user-agent, the web agent
performs session logout in the background and then continues processing access to the current URL.
(property: com.forgerock.agents.config.logout.redirect.disable)",
          "propertyOrder" : 30510,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "policyEvaluationApplication" : {
          "title" : "Policy Set",
          "description" : "Which application contains the policies to evaluate with. (property name:
org.forgerock.openam.agents.config.policy.evaluation.application)",
          "propertyOrder" : 31400,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "ssoWebAgentConfig" : {
      "type" : "object",
      "title" : "SSO",
      "propertyOrder" : 2,
      "properties" : {
        "cookieName" : {
          "title" : "Cookie Name",
          "description" : "Name of the SSO Token cookie used between the AM server and the Agent.
(property name: com.sun.identity.agents.config.cookie.name)<br>Required Agent Restart",
          "propertyOrder" : 29100,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "persistentJwtCookie" : {
          "title" : "Persistent JWT Cookie",
          "description" : "Enable persistence for JWT cookie. If true JWT cookie will not be set as
Session Cookie. (property: org.forgerock.agents.config.cdsso.persistent.cookie.enable)",
          "propertyOrder" : 29270,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "cdssoRedirectUri" : {
          "title" : "CDSSO Redirect URI",
          "description" : "An intermediate URI that is used by the Agent for processing CDSSO
requests. (property name: org.forgerock.agents.authn.redirect.uri) ",
          "propertyOrder" : 29300,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "cookieResetOnRedirect" : {
          "title" : "Session Cookie Reset on Authentication Redirect",
          "description" : "When set to true. the agent will not reset the session cookie on an
authentication redirect if there is a policy advice present.By default, the agent resets the session
cookie in all configured domains on every authentication redirect when a policy advice is present.
(property: org.forgerock.agents.config.cdsso.advice.cleanup.disable)",
          "propertyOrder" : 29400,
          "required" : false,
```

```
          "type" : "boolean",
          "exampleValue" : ""
        },
        "cookieResetEnabled" : {
          "title" : "Cookie Reset",
          "description" : "Agent resets cookies in the response before redirecting to authentication.
(property name: com.sun.identity.agents.config.cookie.reset.enable)",
          "propertyOrder" : 29700,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "secureCookies" : {
          "title" : "Cookie Security",
          "description" : "Agent sends secure cookies if communication is secure. (property name:
com.sun.identity.agents.config.cookie.secure) <br>Required Agent Restart",
          "propertyOrder" : 29200,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "acceptSsoToken" : {
          "title" : "Accept SSO Token",
          "description" : "Specifies whether the agent should accept SSO tokens as session
cookies alongside with ID tokens. Possible values: <br>- false. The agent does not accept SSO
Tokens <br>- true. The agent accepts both SSO tokens and ID tokens as session tokens during
the login flow, and afterwards. SSO tokens are not converted to ID tokens <br>Set this property
to \"true\" only for specific migration cases (see documentation for more info) <br>(property:
com.forgerock.agents.accept.sso.token) (Agent 5.7+ only)",
          "propertyOrder" : 29850,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "httpOnly" : {
          "title" : "HTTP Only Mode",
          "description" : "Agents with this property set to true mark cookies as HTTPOnly
to prevent scripts and third-party programs from accessing the cookies. (property:
com.sun.identity.cookie.httponly)",
          "propertyOrder" : 29250,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "multivaluePreAuthnCookie" : {
          "title" : "Multivalue for Pre-Authn Cookie",
          "description" : "With this set, the agent will use a legacy mode to create cookies that are
used to track unauthenticated requests that have been redirected to login. This mode should only be
used for backward compatibility, where the pre-5.7 way of tracking redirected requests is required,
perhaps because the cookie names are referenced in proxy configuration. This property need not be set
in any other situation. (property: org.forgerock.openam.agents.config.multivalue.pre.authn.cookies)",
          "propertyOrder" : 29280,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "cookieResetList" : {
          "title" : "Cookies Reset Name List",
```

```
          "description" : "List of cookies in the format: name[=value][;Domain=value].
(property name: com.sun.identity.agents.config.cookie.reset) <br> Examples: <br> Cookie1 <br>
Cookie2=value;Domain=subdomain.domain.com",
          "propertyOrder" : 29800,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "sameSite" : {
          "title" : "SameSite Cookie Attribute",
          "description" : "If set, agent will add SameSite attribute to all cookies created by
agent with value which is provided in this property. <br>Example: Strict, Lax, None (property:
com.forgerock.agents.cdsso.cookie.samesite)",
          "propertyOrder" : 29260,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "cdssoCookieDomain" : {
          "title" : "Cookies Domain List",
          "description" : "List of domains in which cookies have to be set in CDSSO. (property name:
com.sun.identity.agents.config.cdsso.cookie.domain) <br> Example: <br> .example.com",
          "propertyOrder" : 29600,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        }
      }
    },
    "advancedWebAgentConfig" : {
      "type" : "object",
      "title" : "Advanced",
      "propertyOrder" : 5,
      "properties" : {
        "pdpStickySessionMode" : {
          "title" : "POST Data Sticky Load Balancing Mode",
          "description" : "Specifies whether to create a cookie, or to append a
query string to the URL to assist with sticky load balancing. Possible values
are: <br>COOKIE. The web agent creates a cookie with the value specified
in the com.sun.identity.agents.config.postdata.preserve.stickysession.value
property. <br>URL. The web agent appends the value specified in the
com.sun.identity.agents.config.postdata.preserve.stickysession.value to the URL query string. <br>
(property: com.sun.identity.agents.config.postdata.preserve.stickysession.mode)",
          "propertyOrder" : 33700,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "pdpStickySessionValue" : {
          "title" : "POST Data Sticky Load Balancing Value",
          "description" : "Specifies a key-value pair separated by the = character that the web
agent creates when evaluating the \"POST Data Sticky Load Balancing Mode\". For example, a setting
of lb=myserver either sets an lb cookie with myserver value, or adds lb=myserver to the URL query
```

```
string. When configuring POST data preservation with cookies, set the cookie name in the cookie
pair to the same value configured in the \"POST Data Sticky Load Balancing Cookie Name\". (property:
com.sun.identity.agents.config.postdata.preserve.stickysession.value)",
          "propertyOrder" : 33710,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "logonAndImpersonation" : {
          "title" : "Logon and Impersonation",
          "description" : "Set to true if agent should do Windows Logon and User Impersonation.
(property name: com.sun.identity.agents.config.iis.logonuser)",
          "propertyOrder" : 34500,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "clientHostnameHeader" : {
          "title" : "Client Hostname Header",
          "description" : "HTTP header name that holds the Hostname of the client. (property name:
org.forgerock.agents.http.header.containing.remote.hostname) ",
          "propertyOrder" : 32900,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "fragmentRedirectEnabled" : {
          "title" : "Fragment Redirect Enabled",
          "description" : "Enable to save the browser's URL fragment during authentication.
<br>(property: org.forgerock.agents.config.fragment.redirect.enable) (Agent 5.7+ only)",
          "propertyOrder" : 33400,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "postDataPreservation" : {
          "title" : "POST Data Preservation",
          "description" : "Enables POST data preservation. (property name:
com.sun.identity.agents.config.postdata.preserve.enable) <br> Note that this feature is not supported
in all the web agents. Please refer individual agents documentation for more details.",
          "propertyOrder" : 33500,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "overrideRequestPort" : {
          "title" : "Override Request URL Port",
          "description" : "Set to true if the agent is sitting behind a ssl/tls
off-loader, load balancer, or proxy to override the port with the value from
the property com.sun.identity.agents.config.agenturi.prefix. (property name:
com.sun.identity.agents.config.override.port)",
          "propertyOrder" : 33300,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "pdpJavascriptRepost" : {
          "title" : "Show Password in HTTP Header",
```

```
          "description" : "Set to true if encrypted password should be set in HTTP header
AUTH_PASSWORD. (property name: com.sun.identity.agents.config.iis.password.header)",
          "propertyOrder" : 33730,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "clientIpHeader" : {
          "title" : "Client IP Address Header",
          "description" : "HTTP header name that holds the IP address of the client. (property name:
org.forgerock.agents.http.header.containing.ip.address) ",
          "propertyOrder" : 32800,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "postDataCachePeriod" : {
          "title" : "POST Data Entries Cache Period",
          "description" : "POST cache entry lifetime in minutes. (property name:
com.sun.identity.agents.config.postcache.entry.lifetime)",
          "propertyOrder" : 33600,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "replayPasswordKey" : {
          "title" : "Replay Password Key",
          "description" : "DES key for decrypting the basic authentication password in the session.
(property name: com.sun.identity.agents.config.replaypasswd.key)",
          "propertyOrder" : 33900,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "customProperties" : {
          "title" : "Custom Properties",
          "description" : "Additional properties that allow users to augment the set of
properties supported by agent. (property name: com.sun.identity.agents.config.freeformproperties)
 <br> Examples: <br> customproperty=custom-value1 <br> customlist[0]=customlist-value-0
<br> customlist[1]=customlist-value-1 <br> custommap[key1]=custommap-value-1 <br>
custommap[key2]=custommap-value-2",
          "propertyOrder" : 35100,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "overrideRequestProtocol" : {
          "title" : "Override Request URL Protocol",
          "description" : "Set to true if the agent is sitting behind a ssl/tls
off-loader, load balancer, or proxy to override the protocol with the value from
the property com.sun.identity.agents.config.agenturi.prefix. (property name:
com.sun.identity.agents.config.override.protocol)",
          "propertyOrder" : 33100,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
```

```
        },
        "showPasswordInHeader" : {
          "title" : "Show Password in HTTP Header",
          "description" : "Set to true if encrypted password should be set in HTTP header
 AUTH_PASSWORD. (property name: com.sun.identity.agents.config.iis.password.header)",
          "propertyOrder" : 34400,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "pdpStickySessionCookieName" : {
          "title" : "POST Data Sticky Load Balancing Cookie Name",
          "description" : "Specifies the name of a cookie to use for enabling sticky load balancing
 when the \"POST Data Sticky Load Balancing Mode\" property is set to COOKIE. Set the cookie name
 to the same value configured in the \"POST Data Sticky Load Balancing Value\" property. (property:
 com.sun.identity.agents.config.postdata.preserve.lbcookie)",
          "propertyOrder" : 33720,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "overrideRequestHost" : {
          "title" : "Override Request URL Host",
          "description" : "Set to true if the agent is sitting behind a ssl/tls
 off-loader, load balancer, or proxy to override the host with the value from
 the property com.sun.identity.agents.config.agenturi.prefix. (property name:
 com.sun.identity.agents.config.override.host)",
          "propertyOrder" : 33200,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "pdpSkipPostUrl" : {
          "title" : "URLs Ignored by the Agent POST Data Inspector",
          "description" : "Specifies a list of URLs that will not be processed by the web agent
 POST data inspector. This allows other modules on the same server to access the POST data directly.
 <br>The following example uses wildcards to add a file named postreader.jsp in the root of any
 protected website to the list of URLs that will not have their POST data inspected: <br>http*://*:*/
postreader.jsp <br>Any URLs added to this property should also be added to the Not-Enforced URLs <br>
 (property: org.forgerock.agents.config.skip.post.url)",
          "propertyOrder" : 33740,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        }
      }
    },
    "miscWebAgentConfig" : {
      "type" : "object",
      "title" : "Miscellaneous",
      "propertyOrder" : 4,
      "properties" : {
        "addCacheControlHeader" : {
          "title" : "Add Cache-Control Headers",
```

```
          "description" : "Set this property to true to enable use of Cache-Control headers
 that prevent proxies from caching resources accessed by unauthenticated users. (property:
 com.forgerock.agents.cache_control_header.enable)",
          "propertyOrder" : 32710,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "urlJsonResponse" : {
          "title" : "URLs to Receive JSON-Formatted Responses",
          "description" : "Returning the responses in JSON format is useful for non-
browser-based, or AJAX applications, that may not want to redirect users to the AM user
 interface for authentication. <br>Example: org.forgerock.agents.config.json.url[0]=http*://
*.example.com:*/api/* <br>org.forgerock.agents.config.json.response.code=202 <br>(property:
 org.forgerock.agents.config.json.url)",
          "propertyOrder" : 32730,
          "required" : false,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "anonymousUserId" : {
          "title" : "Anonymous User Default Value",
          "description" : "User id of unauthenticated users. (property name:
 com.sun.identity.agents.config.anonymous.user.id)",
          "propertyOrder" : 32700,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "statusCodeJsonResponse" : {
          "title" : "HTTP Return Code for JSON-Formatted Responses",
          "description" : "Specifies an HTTP response code to return when a JSON-formatted error is
 triggered. (property: org.forgerock.agents.config.json.response.code)",
          "propertyOrder" : 32760,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        },
        "encodeUrlSpecialCharacters" : {
          "title" : "Encode URL's Special Characters",
          "description" : "Encodes the url which has special characters before doing policy
 evaluation. (property name: com.sun.identity.agents.config.encode.url.special.chars.enable)",
          "propertyOrder" : 32100,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "mineEncodeHeader" : {
          "title" : "MIME-Encode HTTP Header Values",
          "description" : "Specifies whether the agent must MIME-encode HTTP header values, and
 when to do it. Possible values are: <br>  0. The agent MIME-encodes the value of HTTP headers
 if said value is a multi-byte Unicode string. <br>  1. The agent MIME-encodes the value of every
 HTTP header. <br>  2. The agent does not MIME-encode the value of any HTTP header. <br> (property:
 com.forgerock.agents.header.mime.encode)",
          "propertyOrder" : 32720,
          "required" : false,
```

```
          "type" : "integer",
          "exampleValue" : ""
        },
        "compositeAdviceEncode" : {
          "title" : "Composite Advice Encode",
          "description" : "This property is used to specify whether AM composite advices
should be based64url encoded before sending to custom login endpoints. (property:
com.forgerock.agents.advice.b64.url.encode)",
          "propertyOrder" : 32300,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "compositeAdviceRedirect" : {
          "title" : "Composite Advice Handling",
          "description" : "When set to true, the agent sends composite advice in
the query (GET request) instead of sending it through a POST request. (property:
com.sun.am.use_redirect_for_advice)",
          "propertyOrder" : 32200,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "ignorePathInfo" : {
          "title" : "Ignore Path Info in Request URL",
          "description" : "The path info will be stripped from the request URL while doing Not
Enforced List check and url policy evaluation if the value is set to true. (property name:
com.sun.identity.agents.config.ignore.path.info)",
          "propertyOrder" : 32400,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "gotoParameterName" : {
          "title" : "Goto Parameter Name",
          "description" : "This is the name of the HTTP query \"goto\" parameter. It is not
recommended to change it. (property name: com.sun.identity.agents.config.redirect.param) ",
          "propertyOrder" : 32600,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "invertUrlJsonResponse" : {
          "title" : "Invert Properties That Receive JSON-Formatted Responses",
          "description" : "Set to true to invert the meaning of both the
org.forgerock.agents.config.json.url and org.forgerock.agents.config.json.header properties.
When inverted the specified values in those two properties will not trigger JSON-formatted
responses. Any non-specified value will trigger JSON-formatted responses, instead. (property:
org.forgerock.agents.config.json.url.invert)",
          "propertyOrder" : 32750,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "invalidUrlRegex" : {
          "title" : "Invalid URL Regular Expression",
          "description" : "Specifies a Perl-compatible regular expression to parse valid request
URLs. The web agent rejects requests to invalid URLs with HTTP 403 Forbidden status without
further processing. <br>Example, to filter out URLs containing a list of characters and words
```

```
such as ./ /. / . %00-%1f, %7f-%ff, %25, %2B, %2C, %7E, .info, configure the following regular
expression: <br>^(\\?!.\\/|\\/.|.|.info|%2B|%00-%1f|%7f-%ff|%25|%2C|%7E).*$ <br>(property:
com.forgerock.agents.agent.invalid.url.regex)",
          "propertyOrder" : 32500,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "profileAttributesCookiePrefix" : {
          "title" : "Profile Attributes Cookie Prefix",
          "description" : "Sets cookie prefix in the attributes headers. (property name:
com.sun.identity.agents.config.profile.attribute.cookie.prefix)",
          "propertyOrder" : 31800,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "headerJsonResponse" : {
          "title" : "Headers and Values to Receive JSON-Formatted Responses",
          "description" : "Specify HTTP headers and associated values
that trigger JSON-formatted errors to be returned. <br>Example:
<br>org.forgerock.agents.config.json.header[enableJsonResponse]=true
<br>org.forgerock.agents.config.json.response.code=202 <br>(property:
org.forgerock.agents.config.json.header[Header]=Value)",
          "propertyOrder" : 32740,
          "required" : false,
          "patternProperties" : {
            ".*" : {
              "type" : "string"
            }
          },
          "type" : "object",
          "exampleValue" : ""
        },
        "encodeSpecialCharsInCookies" : {
          "title" : "Encode special chars in Cookies",
          "description" : "Encode special chars in cookie by URL encoding. Useful when profile,
session and response attributes contain special chars and attributes fetch mode is set to
HTTP_COOKIE. (property name: com.sun.identity.agents.config.encode.cookie.special.chars.enable)  ",
          "propertyOrder" : 31700,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "caseInsensitiveUrlComparison" : {
          "title" : "URL Comparison Case Sensitivity Check",
          "description" : "Enforces case insensitivity in both policy and not enforced url evaluation.
(property name: com.sun.identity.agents.config.url.comparison.case.ignore)",
          "propertyOrder" : 32000,
          "required" : false,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "anonymousUserEnabled" : {
          "title" : "Anonymous User",
          "description" : "Enable/Disable REMOTE_USER processing for anonymous users. (property name:
com.sun.identity.agents.config.anonymous.user.enable)",
          "propertyOrder" : 31600,
          "required" : false,
```

```
          "type" : "boolean",
          "exampleValue" : ""
        },
        "profileAttributesCookieMaxAge" : {
          "title" : "Profile Attributes Cookie Maxage",
          "description" : "Maxage of attributes cookie headers. (property name:
 com.sun.identity.agents.config.profile.attribute.cookie.maxage)",
          "propertyOrder" : 31900,
          "required" : false,
          "type" : "integer",
          "exampleValue" : ""
        }
      }
    }
  }
}
```

WebAgents

Realm Operations

Agents handler that is responsible for managing agents

Resource path: `/realm-config/agents/WebAgent`

Resource version: `1.0`

create

Usage:

```
am> create WebAgents --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "ssoWebAgentConfig" : {
      "type" : "object",
      "title" : "SSO",
      "propertyOrder" : 2,
      "properties" : {
        "cdssoCookieDomain" : {
```

```
          "title" : "Cookies Domain List",
          "description" : "List of domains in which cookies have to be set in CDSSO. (property name:
com.sun.identity.agents.config.cdsso.cookie.domain) <br> Example: <br> .example.com",
          "propertyOrder" : 29600,
          "items" : {
            "type" : "string"
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "array",
              "required" : false
            }
          }
        },
        "acceptSsoToken" : {
          "title" : "Accept SSO Token",
          "description" : "Specifies whether the agent should accept SSO tokens as session
cookies alongside with ID tokens. Possible values: <br>- false. The agent does not accept SSO
Tokens <br>- true. The agent accepts both SSO tokens and ID tokens as session tokens during
the login flow, and afterwards. SSO tokens are not converted to ID tokens <br>Set this property
to \"true\" only for specific migration cases (see documentation for more info) <br>(property:
com.forgerock.agents.accept.sso.token) (Agent 5.7+ only)",
          "propertyOrder" : 29850,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : false
            }
          }
        },
        "multivaluePreAuthnCookie" : {
          "title" : "Multivalue for Pre-Authn Cookie",
          "description" : "With this set, the agent will use a legacy mode to create cookies that are
used to track unauthenticated requests that have been redirected to login. This mode should only be
used for backward compatibility, where the pre-5.7 way of tracking redirected requests is required,
perhaps because the cookie names are referenced in proxy configuration. This property need not be set
in any other situation. (property: org.forgerock.openam.agents.config.multivalue.pre.authn.cookies)",
          "propertyOrder" : 29280,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
```

```
              "required" : false
            }
          }
        },
        "httpOnly" : {
          "title" : "HTTP Only Mode",
          "description" : "Agents with this property set to true mark cookies as HTTPOnly
to prevent scripts and third-party programs from accessing the cookies. (property:
com.sun.identity.cookie.httponly)",
          "propertyOrder" : 29250,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : false
            }
          }
        },
        "secureCookies" : {
          "title" : "Cookie Security",
          "description" : "Agent sends secure cookies if communication is secure. (property name:
com.sun.identity.agents.config.cookie.secure) <br>Required Agent Restart",
          "propertyOrder" : 29200,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : false
            }
          }
        },
        "cookieResetList" : {
          "title" : "Cookies Reset Name List",
          "description" : "List of cookies in the format: name[=value][;Domain=value].
(property name: com.sun.identity.agents.config.cookie.reset) <br> Examples: <br> Cookie1 <br>
Cookie2=value;Domain=subdomain.domain.com",
          "propertyOrder" : 29800,
          "items" : {
            "type" : "string"
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "array",
```

```
              "required" : false
            }
          }
        },
        "cdssoRedirectUri" : {
          "title" : "CDSSO Redirect URI",
          "description" : "An intermediate URI that is used by the Agent for processing CDSSO
requests. (property name: org.forgerock.agents.authn.redirect.uri) ",
          "propertyOrder" : 29300,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "sameSite" : {
          "title" : "SameSite Cookie Attribute",
          "description" : "If set, agent will add SameSite attribute to all cookies created by
agent with value which is provided in this property. <br>Example: Strict, Lax, None (property:
com.forgerock.agents.cdsso.cookie.samesite)",
          "propertyOrder" : 29260,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "cookieResetOnRedirect" : {
          "title" : "Session Cookie Reset on Authentication Redirect",
          "description" : "When set to true. the agent will not reset the session cookie on an
authentication redirect if there is a policy advice present.By default, the agent resets the session
cookie in all configured domains on every authentication redirect when a policy advice is present.
(property: org.forgerock.agents.config.cdsso.advice.cleanup.disable)",
          "propertyOrder" : 29400,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : false
            }
```

```
        }
      },
      "cookieResetEnabled" : {
        "title" : "Cookie Reset",
        "description" : "Agent resets cookies in the response before redirecting to authentication.
(property name: com.sun.identity.agents.config.cookie.reset.enable)",
        "propertyOrder" : 29700,
        "type" : "object",
        "exampleValue" : "",
        "properties" : {
          "inherited" : {
            "type" : "boolean",
            "required" : true
          },
          "value" : {
            "type" : "boolean",
            "required" : false
          }
        }
      },
      "persistentJwtCookie" : {
        "title" : "Persistent JWT Cookie",
        "description" : "Enable persistence for JWT cookie. If true JWT cookie will not be set as
Session Cookie. (property: org.forgerock.agents.config.cdsso.persistent.cookie.enable)",
        "propertyOrder" : 29270,
        "type" : "object",
        "exampleValue" : "",
        "properties" : {
          "inherited" : {
            "type" : "boolean",
            "required" : true
          },
          "value" : {
            "type" : "boolean",
            "required" : false
          }
        }
      },
      "cookieName" : {
        "title" : "Cookie Name",
        "description" : "Name of the SSO Token cookie used between the AM server and the Agent.
(property name: com.sun.identity.agents.config.cookie.name)<br>Required Agent Restart",
        "propertyOrder" : 29100,
        "type" : "object",
        "exampleValue" : "",
        "properties" : {
          "inherited" : {
            "type" : "boolean",
            "required" : true
          },
          "value" : {
            "type" : "string",
            "required" : false
          }
        }
      }
    }
  },
  "amServicesWebAgent" : {
```

```
      "type" : "object",
      "title" : "AM Services",
      "propertyOrder" : 3,
      "properties" : {
        "fetchPoliciesFromRootResource" : {
          "title" : "Fetch Policies from Root Resource",
          "description" : "Agent caches policy decision of the resource and all resources from the
root of the resource down. (property name: com.sun.identity.agents.config.fetch.from.root.resource)
<br>Required Agent Restart",
          "propertyOrder" : 31000,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : false
            }
          }
        },
        "userIdParameterType" : {
          "title" : "User ID Parameter Type",
          "description" : "User ID can be fetched from either SESSION and LDAP attributes. (property
name: com.sun.identity.agents.config.userid.param.type)",
          "propertyOrder" : 30900,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "logoutUrlRegex" : {
          "title" : "Logout URL Regular Expression",
          "description" : "Perl-compatible regular expression that matches logout URLs. For
example, to match URLs with protectedA or protectedB in the path and op=logout in the query
string, use the following setting: <br>*(/protectedA\\?|/protectedB\\?/).*(\\&op=logout\\&)(.*|$)
 <br>When you use this property, the agent ignores the settings for Logout URL List. (property:
com.forgerock.agents.agent.logout.url.regex)",
          "propertyOrder" : 30540,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
```

```
            }
          }
        },
        "regexConditionalLoginUrl" : {
          "title" : "Regular Expression Conditional Login URL",
          "description" : "Conditionally redirect users based on the incoming request URL. If the
 incoming request URL matches a regular expression, the web agent redirects the request to a specific
 URL. That specific URL can be an AM instance, site, or a different website. Specifies the redirection
 URL and its parameters. This property needs to configure \"Regular Expression Conditional Login
 Pattern\" <br>Example: <br>  org.forgerock.agents.config.conditional.login.pattern[0] = .*shop <br>
  org.forgerock.agents.config.conditional.login.url[0] = http://openam.example.com/openam/oauth2/
authorize?realm=sales <br>(property: org.forgerock.agents.config.conditional.login.url)",
          "propertyOrder" : 30100,
          "items" : {
            "type" : "string"
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "array",
              "required" : false
            }
          }
        },
        "policyCachePollingInterval" : {
          "title" : "Policy Cache Polling Period",
          "description" : "Polling interval in minutes to refresh agent's policy cache. (property
 name: com.sun.identity.agents.config.policy.cache.polling.interval) <br>Required Agent Restart",
          "propertyOrder" : 30600,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "integer",
              "required" : false
            }
          }
        },
        "amLogoutUrl" : {
          "title" : "AM Logout URL",
          "description" : "AM logout page URL. (property name:
 com.sun.identity.agents.config.logout.url)  <br> Example: <br> http://host:port/am/UI/Logout",
          "propertyOrder" : 30200,
          "items" : {
            "type" : "string"
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
```

```
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "array",
              "required" : false
            }
          }
        },
        "userIdParameter" : {
          "title" : "User ID Parameter",
          "description" : "Agent sets value of User Id to REMOTE_USER server variable. (property name:
com.sun.identity.agents.config.userid.param)",
          "propertyOrder" : 30800,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "publicAmUrl" : {
          "title" : "Public AM URL",
          "description" : "Overrides the agent's behavior of finding a suitable AM server and
specifies the public URL of the AM to redirect to. <br> Use this property if: <br>  - Your
environment uses custom login pages (OIDC-compliant and non-OIDC-compliant flows). <br>  - Your
environment's custom login pages are in a network that can only access AM using a proxy, a firewall,
or any other technology that remaps the AM URL to one accessible by the custom login pages. <br>
 -End-users cannot log in due to their cookies being set in the wrong domains. <br>(property:
com.forgerock.agents.public.am.url) ",
          "propertyOrder" : 29950,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "applicationLogoutUrls" : {
          "title" : "Logout URL List",
          "description" : "List of application logout URLs. User gets logged out from AM session
when these urls accessed. (property name: com.sun.identity.agents.config.agent.logout.url). If
this property is used, user should specify a value for the below Logout Redirect URL property. <br>
Example: <br> http://myagent.mydomain.com/logout.html",
          "propertyOrder" : 30300,
          "items" : {
            "type" : "string"
```

```
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "array",
              "required" : false
            }
          }
        },
        "logoutRedirectUrl" : {
          "title" : "Logout Redirect URL",
          "description" : "User gets redirected to this url after logout. (property name:
com.sun.identity.agents.config.logout.redirect.url). This property should be specified along with the
above Logout URL List.",
          "propertyOrder" : 30500,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "policyEvaluationRealm" : {
          "title" : "Policy Evaluation Realm",
          "description" : "Which realm to start evaluating from. (property name:
org.forgerock.openam.agents.config.policy.evaluation.realm)",
          "propertyOrder" : 31300,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "retrieveClientHostname" : {
          "title" : "Retrieve Client Hostname",
          "description" : "Gets the client's hostname through DNS reverse lookup for use in policy
evaluation. (property name: com.sun.identity.agents.config.get.client.host.name)",
          "propertyOrder" : 31100,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
```

```
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : false
            }
          }
        },
        "logoutRedirectDisabled" : {
          "title" : "Disabled Logout Redirection",
          "description" : "When disabled, instead of redirecting the user-agent, the web agent
performs session logout in the background and then continues processing access to the current URL.
(property: com.forgerock.agents.config.logout.redirect.disable)",
          "propertyOrder" : 30510,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : false
            }
          }
        },
        "customLoginMode" : {
          "title" : "Custom Login Mode",
          "description" : "Specifies whether the agent should use the default or the custom login
mode when redirecting unauthenticated users.<br>Possible values are: <br>0. Disabled. Default login
redirection mode enabled <br>  1. Custom login mode enabled based on converts the SSO token into an
ID token <br>  2. Legacy Custom login mode. Can be used in specific migration cases from agent 4
<br>(property: org.forgerock.openam.agents.config.allow.custom.login)",
          "propertyOrder" : 29890,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "integer",
              "required" : false
            }
          }
        },
        "logoutResetCookies" : {
          "title" : "Logout Cookies List for Reset",
          "description" : "Any cookies to be reset upon logout in the same format as cookie reset
list. (property name: com.sun.identity.agents.config.logout.cookie.reset) <br> Cookie1 <br>
Cookie2=value;Domain=subdomain.domain.com",
          "propertyOrder" : 30400,
          "items" : {
            "type" : "string"
          },
```

```
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "array",
              "required" : false
            }
          }
        },
        "policyEvaluationApplication" : {
          "title" : "Policy Set",
          "description" : "Which application contains the policies to evaluate with. (property name:
org.forgerock.openam.agents.config.policy.evaluation.application)",
          "propertyOrder" : 31400,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "conditionalLoginUrl" : {
          "title" : "AM Conditional Login URL",
          "description" : "Conditionally redirect users based on the incoming request URL. If
the incoming request URL matches a specified domain name, the web agent redirects the request
to a specific URL. That specific URL can be an AM instance, site, or a different website.
<br>Example: <br>  example.com|https://openam.example.com/openam/oauth2/authorize <br>
myapp.domain.com|https://openam2.example.com/openam/oauth2/authorize?realm=sales (property:
com.forgerock.agents.conditional.login.url)",
          "propertyOrder" : 30000,
          "items" : {
            "type" : "string"
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "array",
              "required" : false
            }
          }
        },
        "regexConditionalLoginPattern" : {
          "title" : "Regular Expression Conditional Login Pattern",
```

```
          "description" : "Conditionally redirect users based on the incoming request
 URL. If the incoming request URL matches a regular expression, the web agent redirects
 the request to a specific URL. That specific URL can be an AM instance, site, or
 a different website. Specifies the regular expression that the domain name must
 match. This property needs to configure \"Regular Expression Conditional Login URL\"
 <br>Example: <br>  org.forgerock.agents.config.conditional.login.pattern[0] = .*shop <br>
 org.forgerock.agents.config.conditional.login.url[0] = http://openam.example.com/openam/oauth2/
authorize?realm=sales <br>(property: org.forgerock.agents.config.conditional.login.pattern)",
          "propertyOrder" : 30050,
          "items" : {
            "type" : "string"
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "array",
              "required" : false
            }
          }
        },
        "amLoginUrl" : {
          "title" : "AM Login URL",
          "description" : "AM login page URL. (property name:
 com.sun.identity.agents.config.login.url)  <br> Example: <br> http://host:port/am/UI/Login",
          "propertyOrder" : 29900,
          "items" : {
            "type" : "string"
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "array",
              "required" : false
            }
          }
        },
        "invalidateLogoutSession" : {
          "title" : "Invalidate Logout Session",
          "description" : "Specifies whether the agent must invalidate the
 user session in AM when redirecting to the logout URL specified either by the
 Logout URL list (com.sun.identity.agents.config.agent.logout.url) or the AM
 logout URL (com.sun.identity.agents.config.logout.url) properties. (property:
 org.forgerock.agents.config.logout.session.invalidate)",
          "propertyOrder" : 30520,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
```

```
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : false
            }
          }
        },
        "policyClockSkew" : {
          "title" : "Policy Clock Skew",
          "description" : "Time in seconds used adjust time difference between Agent
machine and AM. Clock skew in seconds = AgentTime - AMServerTime. (property name:
com.sun.identity.agents.config.policy.clock.skew) <br>Required Agent Restart",
          "propertyOrder" : 31200,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "integer",
              "required" : false
            }
          }
        },
        "ssoCachePollingInterval" : {
          "title" : "SSO Cache Polling Period",
          "description" : "Polling interval in minutes to refresh agent's sso cache. (property name:
com.sun.identity.agents.config.sso.cache.polling.interval) <br>Required Agent Restart",
          "propertyOrder" : 30700,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "integer",
              "required" : false
            }
          }
        },
        "enableLogoutRegex" : {
          "title" : "Enable Regex for Logout URL List",
          "description" : "This property allows regular expressions in \"Logout URL List\" (property:
org.forgerock.agents.config.logout.regex.enable)",
          "propertyOrder" : 30530,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
```

```
              "required" : false
            }
          }
        }
      }
    },
    "globalWebAgentConfig" : {
      "type" : "object",
      "title" : "Global",
      "propertyOrder" : 0,
      "properties" : {
        "status" : {
          "title" : "Status",
          "description" : "Status of the agent configuration.",
          "propertyOrder" : 25100,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : true
            }
          }
        },
        "agentConfigChangeNotificationsEnabled" : {
          "title" : "Agent Configuration Change Notification",
          "description" : "Enable agent to receive notification messages
(via websockets) from AM server for configuration changes. (property name:
org.forgerock.agents.config.change.notifications.enabled) ",
          "propertyOrder" : 25300,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : false
            }
          }
        },
        "jwtName" : {
          "title" : "JWT Cookie Name",
          "description" : "The name used by the agent to set the OIDC JWT on the user's browser.
(property: org.forgerock.agents.jwt.cookie.name)",
          "propertyOrder" : 25500,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
```

```
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "ssoOnlyMode" : {
          "title" : "SSO Only Mode",
          "description" : "Agent will just enforce authentication (SSO), but no authorization for
policies. (property name: com.sun.identity.agents.config.sso.only)",
          "propertyOrder" : 26200,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : false
            }
          }
        },
        "auditLogLocation" : {
          "title" : "Audit Log Location",
          "description" : "Specifies where audit messages should be logged. (property name:
com.sun.identity.agents.config.log.disposition)",
          "propertyOrder" : 26800,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "agentgroup" : {
          "title" : "Group",
          "description" : "Add the agent to a group to allow inheritance of property values from the
group. <br>Changing the group will update inherited property values. <br>Inherited property values
are copied to the agent.",
          "propertyOrder" : 100,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "fqdnDefault" : {
          "title" : "FQDN Default",
          "description" : "Fully qualified hostname that the users should use in order to access
resources. (property name: com.sun.identity.agents.config.fqdn.default)",
          "propertyOrder" : 27400,
          "type" : "object",
          "exampleValue" : "",
```

```
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "resetIdleTime" : {
          "title" : "Reset Idle Timeout",
          "description" : "If the agent is configured in SSO-only mode, the session may unexpectedly
expire in AM due to idle timeout before the user has finished accessing the application. <br>Set
this property to true to refresh the timeout when the user performs an action. <br>When set to
true, the agent makes an additional call to AM, this may cause a performance impact. Configure this
property only if: <br>   The agent is configured in SSO-only mode. <br>   User's sessions are timing
out in AM because they are unexpectedly reaching the maximum idle timeout value. <br>(property:
com.forgerock.agents.call.session.refresh)",
          "propertyOrder" : 26250,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : false
            }
          }
        },
        "agentDebugLevel" : {
          "title" : "Agent Debug Level",
          "description" : "Agent debug level. (property name:
com.sun.identity.agents.config.debug.level)",
          "propertyOrder" : 26400,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "userpassword" : {
          "title" : "Password",
          "description" : "",
          "propertyOrder" : 25000,
          "required" : true,
          "type" : "string",
          "format" : "password",
```

```
          "exampleValue" : ""
        },
        "accessDeniedUrl" : {
          "title" : "Resources Access Denied URL",
          "description" : "The URL of the customized access denied page. (property name:
com.sun.identity.agents.config.access.denied.url)",
          "propertyOrder" : 26300,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "auditAccessType" : {
          "title" : "Audit Access Types",
          "description" : "Types of messages to log based on user URL access attempts. (property name:
com.sun.identity.agents.config.audit.accesstype)",
          "propertyOrder" : 26700,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "notificationsEnabled" : {
          "title" : "Enable Notifications",
          "description" : "The notifications help in maintaining agent's sso, policy and configuration
caches. (property name: com.sun.identity.agents.config.notification.enable) <br>Required Agent
Restart",
          "propertyOrder" : 25600,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : false
            }
          }
        },
        "fqdnMapping" : {
          "title" : "FQDN Virtual Host Map",
```

```
          "description" : "Maps virtual, invalid, or partial hostnames, and IP addresses to the FQDN
to access protected resources. (property name: com.sun.identity.agents.config.fqdn.mapping) <br>
Examples: <br>  To map the partial hostname myserver to myserver.mydomain.com: enter myserver in the
Map Key field and myserver.mydomain.com in the Corresponding Map Value field. To map a virtual server
rst.hostname.com that points to the actual server abc.hostname.com: enter valid1 in the Map Key field
and rst.hostname.com in the Corresponding Map Value field.",
          "propertyOrder" : 27500,
          "patternProperties" : {
            ".*" : {
              "type" : "string"
            }
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "object",
              "required" : false
            }
          }
        },
        "configurationPollingInterval" : {
          "title" : "Configuration Reload Interval",
          "description" : "Interval in minutes to fetch agent configuration from AM. (property name:
com.sun.identity.agents.config.polling.interval) <br>Required Agent Restart",
          "propertyOrder" : 25900,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "integer",
              "required" : false
            }
          }
        },
        "cdssoRootUrl" : {
          "title" : "Agent Root URL for CDSSO",
          "description" : "The agent root URL for CDSSO. The valid value is in the following format:
<br>protocol://hostname:port/<br> The protocol represents the protocol used, such as http or https.
The hostname represents the host name of the machine on which the agent resides. The port represents
the port number on which the agent is installed. The slash following the port number is required.",
          "propertyOrder" : 26100,
          "items" : {
            "type" : "string"
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
```

```
            },
            "value" : {
              "type" : "array",
              "required" : false
            }
          }
        },
        "fqdnCheck" : {
          "title" : "FQDN Check",
          "description" : "Enables checking of fqdn default value and fqdn map values. (property name:
com.sun.identity.agents.config.fqdn.check.enable)",
          "propertyOrder" : 27300,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : false
            }
          }
        },
        "jwtAuditWhitelist" : {
          "title" : "Agent Profile ID Whitelist",
          "description" : "Specifies a comma-separated list of profile IDs that the agent will
consider as valid values for the aud claim. This claim is represented in the JWT containing
the end user's session. <br>Example: <br>agentprofile1,agentprofile2,.... <br>When several
agents configured with different agent profiles protect the same application, set this property
to a list of the agent profiles that are protecting the same application. <br>(property:
com.forgerock.agents.jwt.aud.whitelist)",
          "propertyOrder" : 25520,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "webSocketConnectionIntervalInMinutes" : {
          "title" : "Web Socket Connection Interval",
          "description" : "Interval in minutes by which agents reopen their web socket
connection to ensure a fair distribution of connections across AM servers. (property:
org.forgerock.agents.balance.websocket.interval.minutes).",
          "propertyOrder" : 25400,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
```

```
            },
            "value" : {
              "type" : "integer",
              "required" : false
            }
          }
        },
        "disableJwtAudit" : {
          "title" : "Disable validation of the audience claim",
          "description" : "Specifies whether the agent should validate the audience claim matches the
agent profile ID represented in the JWT containing the end user's session. <br>Possible values are:
<br>  false = The agent validates audience claim. <br>  true = The agent does not validate audience
claim.<br> (property: com.forgerock.agents.jwt.aud.disable)",
          "propertyOrder" : 25510,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : false
            }
          }
        },
        "agentUriPrefix" : {
          "title" : "Agent Deployment URI Prefix",
          "description" : "(property name: com.sun.identity.agents.config.agenturi.prefix)",
          "propertyOrder" : 25800,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "repositoryLocation" : {
          "title" : "Location of Agent Configuration Repository",
          "description" : "Indicates agent's configuration located either on agent's host or centrally
on AM server (property: org.forgerock.agents.config.location).",
          "propertyOrder" : 25200,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      }
    },
    "miscWebAgentConfig" : {
      "type" : "object",
      "title" : "Miscellaneous",
      "propertyOrder" : 4,
```

```
     "properties" : {
       "ignorePathInfo" : {
         "title" : "Ignore Path Info in Request URL",
         "description" : "The path info will be stripped from the request URL while doing Not
Enforced List check and url policy evaluation if the value is set to true. (property name:
com.sun.identity.agents.config.ignore.path.info)",
         "propertyOrder" : 32400,
         "type" : "object",
         "exampleValue" : "",
         "properties" : {
           "inherited" : {
             "type" : "boolean",
             "required" : true
           },
           "value" : {
             "type" : "boolean",
             "required" : false
           }
         }
       },
       "invalidUrlRegex" : {
         "title" : "Invalid URL Regular Expression",
         "description" : "Specifies a Perl-compatible regular expression to parse valid request
URLs. The web agent rejects requests to invalid URLs with HTTP 403 Forbidden status without
further processing. <br>Example, to filter out URLs containing a list of characters and words
such as ./ /. / . %00-%1f, %7f-%ff, %25, %2B, %2C, %7E, .info, configure the following regular
expression: <br>^(\\?!.\\/|\\/.|.|.info|%2B|%00-%1f|%7f-%ff|%25|%2C|%7E).*$ <br>(property:
com.forgerock.agents.agent.invalid.url.regex)",
         "propertyOrder" : 32500,
         "type" : "object",
         "exampleValue" : "",
         "properties" : {
           "inherited" : {
             "type" : "boolean",
             "required" : true
           },
           "value" : {
             "type" : "string",
             "required" : false
           }
         }
       },
       "encodeUrlSpecialCharacters" : {
         "title" : "Encode URL's Special Characters",
         "description" : "Encodes the url which has special characters before doing policy
evaluation. (property name: com.sun.identity.agents.config.encode.url.special.chars.enable)",
         "propertyOrder" : 32100,
         "type" : "object",
         "exampleValue" : "",
         "properties" : {
           "inherited" : {
             "type" : "boolean",
             "required" : true
           },
           "value" : {
             "type" : "boolean",
             "required" : false
           }
         }
```

```
      },
      "profileAttributesCookiePrefix" : {
        "title" : "Profile Attributes Cookie Prefix",
        "description" : "Sets cookie prefix in the attributes headers. (property name:
com.sun.identity.agents.config.profile.attribute.cookie.prefix)",
        "propertyOrder" : 31800,
        "type" : "object",
        "exampleValue" : "",
        "properties" : {
          "inherited" : {
            "type" : "boolean",
            "required" : true
          },
          "value" : {
            "type" : "string",
            "required" : false
          }
        }
      },
      "headerJsonResponse" : {
        "title" : "Headers and Values to Receive JSON-Formatted Responses",
        "description" : "Specify HTTP headers and associated values
that trigger JSON-formatted errors to be returned. <br>Example:
<br>org.forgerock.agents.config.json.header[enableJsonResponse]=true
<br>org.forgerock.agents.config.json.response.code=202 <br>(property:
org.forgerock.agents.config.json.header[Header]=Value)",
        "propertyOrder" : 32740,
        "patternProperties" : {
          ".*" : {
            "type" : "string"
          }
        },
        "type" : "object",
        "exampleValue" : "",
        "properties" : {
          "inherited" : {
            "type" : "boolean",
            "required" : true
          },
          "value" : {
            "type" : "object",
            "required" : false
          }
        }
      },
      "anonymousUserId" : {
        "title" : "Anonymous User Default Value",
        "description" : "User id of unauthenticated users. (property name:
com.sun.identity.agents.config.anonymous.user.id)",
        "propertyOrder" : 32700,
        "type" : "object",
        "exampleValue" : "",
        "properties" : {
          "inherited" : {
            "type" : "boolean",
            "required" : true
          },
          "value" : {
            "type" : "string",
```

```
              "required" : false
            }
          }
        },
        "invertUrlJsonResponse" : {
          "title" : "Invert Properties That Receive JSON-Formatted Responses",
          "description" : "Set to true to invert the meaning of both the
org.forgerock.agents.config.json.url and org.forgerock.agents.config.json.header properties.
When inverted the specified values in those two properties will not trigger JSON-formatted
responses. Any non-specified value will trigger JSON-formatted responses, instead. (property:
org.forgerock.agents.config.json.url.invert)",
          "propertyOrder" : 32750,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : false
            }
          }
        },
        "profileAttributesCookieMaxAge" : {
          "title" : "Profile Attributes Cookie Maxage",
          "description" : "Maxage of attributes cookie headers. (property name:
com.sun.identity.agents.config.profile.attribute.cookie.maxage)",
          "propertyOrder" : 31900,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "integer",
              "required" : false
            }
          }
        },
        "anonymousUserEnabled" : {
          "title" : "Anonymous User",
          "description" : "Enable/Disable REMOTE_USER processing for anonymous users. (property name:
com.sun.identity.agents.config.anonymous.user.enable)",
          "propertyOrder" : 31600,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : false
            }
```

```
        }
      },
      "mineEncodeHeader" : {
        "title" : "MIME-Encode HTTP Header Values",
        "description" : "Specifies whether the agent must MIME-encode HTTP header values, and
when to do it. Possible values are: <br>  0. The agent MIME-encodes the value of HTTP headers
if said value is a multi-byte Unicode string. <br>  1. The agent MIME-encodes the value of every
HTTP header. <br>  2. The agent does not MIME-encode the value of any HTTP header. <br> (property:
com.forgerock.agents.header.mime.encode)",
        "propertyOrder" : 32720,
        "type" : "object",
        "exampleValue" : "",
        "properties" : {
          "inherited" : {
            "type" : "boolean",
            "required" : true
          },
          "value" : {
            "type" : "integer",
            "required" : false
          }
        }
      },
      "compositeAdviceEncode" : {
        "title" : "Composite Advice Encode",
        "description" : "This property is used to specify whether AM composite advices
should be based64url encoded before sending to custom login endpoints. (property:
com.forgerock.agents.advice.b64.url.encode)",
        "propertyOrder" : 32300,
        "type" : "object",
        "exampleValue" : "",
        "properties" : {
          "inherited" : {
            "type" : "boolean",
            "required" : true
          },
          "value" : {
            "type" : "boolean",
            "required" : false
          }
        }
      },
      "addCacheControlHeader" : {
        "title" : "Add Cache-Control Headers",
        "description" : "Set this property to true to enable use of Cache-Control headers
that prevent proxies from caching resources accessed by unauthenticated users. (property:
com.forgerock.agents.cache_control_header.enable)",
        "propertyOrder" : 32710,
        "type" : "object",
        "exampleValue" : "",
        "properties" : {
          "inherited" : {
            "type" : "boolean",
            "required" : true
          },
          "value" : {
            "type" : "boolean",
            "required" : false
          }
```

```
          }
        },
        "statusCodeJsonResponse" : {
          "title" : "HTTP Return Code for JSON-Formatted Responses",
          "description" : "Specifies an HTTP response code to return when a JSON-formatted error is
 triggered. (property: org.forgerock.agents.config.json.response.code)",
          "propertyOrder" : 32760,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "integer",
              "required" : false
            }
          }
        },
        "gotoParameterName" : {
          "title" : "Goto Parameter Name",
          "description" : "This is the name of the HTTP query \"goto\" parameter. It is not
 recommended to change it. (property name: com.sun.identity.agents.config.redirect.param) ",
          "propertyOrder" : 32600,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "urlJsonResponse" : {
          "title" : "URLs to Receive JSON-Formatted Responses",
          "description" : "Returning the responses in JSON format is useful for non-
browser-based, or AJAX applications, that may not want to redirect users to the AM user
 interface for authentication. <br>Example: org.forgerock.agents.config.json.url[0]=http*://
*.example.com:*/api/* <br>org.forgerock.agents.config.json.response.code=202 <br>(property:
 org.forgerock.agents.config.json.url)",
          "propertyOrder" : 32730,
          "items" : {
            "type" : "string"
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "array",
              "required" : false
```

```
            }
          }
        },
        "encodeSpecialCharsInCookies" : {
          "title" : "Encode special chars in Cookies",
          "description" : "Encode special chars in cookie by URL encoding. Useful when profile,
session and response attributes contain special chars and attributes fetch mode is set to
HTTP_COOKIE. (property name: com.sun.identity.agents.config.encode.cookie.special.chars.enable)  ",
          "propertyOrder" : 31700,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : false
            }
          }
        },
        "caseInsensitiveUrlComparison" : {
          "title" : "URL Comparison Case Sensitivity Check",
          "description" : "Enforces case insensitivity in both policy and not enforced url evaluation.
(property name: com.sun.identity.agents.config.url.comparison.case.ignore)",
          "propertyOrder" : 32000,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : false
            }
          }
        },
        "compositeAdviceRedirect" : {
          "title" : "Composite Advice Handling",
          "description" : "When set to true, the agent sends composite advice in
the query (GET request) instead of sending it through a POST request. (property:
com.sun.am.use_redirect_for_advice)",
          "propertyOrder" : 32200,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : false
            }
          }
        }
```

```
      }
    },
    "advancedWebAgentConfig" : {
      "type" : "object",
      "title" : "Advanced",
      "propertyOrder" : 5,
      "properties" : {
        "showPasswordInHeader" : {
          "title" : "Show Password in HTTP Header",
          "description" : "Set to true if encrypted password should be set in HTTP header
AUTH_PASSWORD. (property name: com.sun.identity.agents.config.iis.password.header)",
          "propertyOrder" : 34400,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : false
            }
          }
        },
        "logonAndImpersonation" : {
          "title" : "Logon and Impersonation",
          "description" : "Set to true if agent should do Windows Logon and User Impersonation.
(property name: com.sun.identity.agents.config.iis.logonuser)",
          "propertyOrder" : 34500,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : false
            }
          }
        },
        "pdpStickySessionCookieName" : {
          "title" : "POST Data Sticky Load Balancing Cookie Name",
          "description" : "Specifies the name of a cookie to use for enabling sticky load balancing
when the \"POST Data Sticky Load Balancing Mode\" property is set to COOKIE. Set the cookie name
to the same value configured in the \"POST Data Sticky Load Balancing Value\" property. (property:
com.sun.identity.agents.config.postdata.preserve.lbcookie)",
          "propertyOrder" : 33720,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
```

```
              "required" : false
            }
          }
        },
        "pdpSkipPostUrl" : {
          "title" : "URLs Ignored by the Agent POST Data Inspector",
          "description" : "Specifies a list of URLs that will not be processed by the web agent
 POST data inspector. This allows other modules on the same server to access the POST data directly.
 <br>The following example uses wildcards to add a file named postreader.jsp in the root of any
 protected website to the list of URLs that will not have their POST data inspected: <br>http*://*:*/
postreader.jsp <br>Any URLs added to this property should also be added to the Not-Enforced URLs <br>
 (property: org.forgerock.agents.config.skip.post.url)",
          "propertyOrder" : 33740,
          "items" : {
            "type" : "string"
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "array",
              "required" : false
            }
          }
        },
        "postDataPreservation" : {
          "title" : "POST Data Preservation",
          "description" : "Enables POST data preservation. (property name:
 com.sun.identity.agents.config.postdata.preserve.enable) <br> Note that this feature is not supported
 in all the web agents. Please refer individual agents documentation for more details.",
          "propertyOrder" : 33500,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : false
            }
          }
        },
        "overrideRequestProtocol" : {
          "title" : "Override Request URL Protocol",
          "description" : "Set to true if the agent is sitting behind a ssl/tls
 off-loader, load balancer, or proxy to override the protocol with the value from
 the property com.sun.identity.agents.config.agenturi.prefix. (property name:
 com.sun.identity.agents.config.override.protocol)",
          "propertyOrder" : 33100,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
```

```
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : false
            }
          }
        },
        "customProperties" : {
          "title" : "Custom Properties",
          "description" : "Additional properties that allow users to augment the set of
properties supported by agent. (property name: com.sun.identity.agents.config.freeformproperties)
 <br> Examples: <br> customproperty=custom-value1 <br> customlist[0]=customlist-value-0
<br> customlist[1]=customlist-value-1 <br> custommap[key1]=custommap-value-1 <br>
custommap[key2]=custommap-value-2",
          "propertyOrder" : 35100,
          "items" : {
            "type" : "string"
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "array",
              "required" : false
            }
          }
        },
        "pdpStickySessionMode" : {
          "title" : "POST Data Sticky Load Balancing Mode",
          "description" : "Specifies whether to create a cookie, or to append a
query string to the URL to assist with sticky load balancing. Possible values
are: <br>COOKIE. The web agent creates a cookie with the value specified
in the com.sun.identity.agents.config.postdata.preserve.stickysession.value
property. <br>URL. The web agent appends the value specified in the
com.sun.identity.agents.config.postdata.preserve.stickysession.value to the URL query string. <br>
(property: com.sun.identity.agents.config.postdata.preserve.stickysession.mode)",
          "propertyOrder" : 33700,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "fragmentRedirectEnabled" : {
          "title" : "Fragment Redirect Enabled",
```

```
          "description" : "Enable to save the browser's URL fragment during authentication.
<br>(property: org.forgerock.agents.config.fragment.redirect.enable) (Agent 5.7+ only)",
          "propertyOrder" : 33400,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : false
            }
          }
        },
        "overrideRequestPort" : {
          "title" : "Override Request URL Port",
          "description" : "Set to true if the agent is sitting behind a ssl/tls
off-loader, load balancer, or proxy to override the port with the value from
the property com.sun.identity.agents.config.agenturi.prefix. (property name:
com.sun.identity.agents.config.override.port)",
          "propertyOrder" : 33300,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : false
            }
          }
        },
        "postDataCachePeriod" : {
          "title" : "POST Data Entries Cache Period",
          "description" : "POST cache entry lifetime in minutes. (property name:
com.sun.identity.agents.config.postcache.entry.lifetime)",
          "propertyOrder" : 33600,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "integer",
              "required" : false
            }
          }
        },
        "pdpStickySessionValue" : {
          "title" : "POST Data Sticky Load Balancing Value",
          "description" : "Specifies a key-value pair separated by the = character that the web
agent creates when evaluating the \"POST Data Sticky Load Balancing Mode\". For example, a setting
of lb=myserver either sets an lb cookie with myserver value, or adds lb=myserver to the URL query
```

```
string. When configuring POST data preservation with cookies, set the cookie name in the cookie
pair to the same value configured in the \"POST Data Sticky Load Balancing Cookie Name\". (property:
com.sun.identity.agents.config.postdata.preserve.stickysession.value)",
         "propertyOrder" : 33710,
         "type" : "object",
         "exampleValue" : "",
         "properties" : {
           "inherited" : {
             "type" : "boolean",
             "required" : true
           },
           "value" : {
             "type" : "string",
             "required" : false
           }
         }
       },
       "replayPasswordKey" : {
         "title" : "Replay Password Key",
         "description" : "DES key for decrypting the basic authentication password in the session.
(property name: com.sun.identity.agents.config.replaypasswd.key)",
         "propertyOrder" : 33900,
         "type" : "object",
         "exampleValue" : "",
         "properties" : {
           "inherited" : {
             "type" : "boolean",
             "required" : true
           },
           "value" : {
             "type" : "string",
             "required" : false
           }
         }
       },
       "clientIpHeader" : {
         "title" : "Client IP Address Header",
         "description" : "HTTP header name that holds the IP address of the client. (property name:
org.forgerock.agents.http.header.containing.ip.address) ",
         "propertyOrder" : 32800,
         "type" : "object",
         "exampleValue" : "",
         "properties" : {
           "inherited" : {
             "type" : "boolean",
             "required" : true
           },
           "value" : {
             "type" : "string",
             "required" : false
           }
         }
       },
       "clientHostnameHeader" : {
         "title" : "Client Hostname Header",
         "description" : "HTTP header name that holds the Hostname of the client. (property name:
org.forgerock.agents.http.header.containing.remote.hostname) ",
         "propertyOrder" : 32900,
         "type" : "object",
```

```
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "pdpJavascriptRepost" : {
          "title" : "Show Password in HTTP Header",
          "description" : "Set to true if encrypted password should be set in HTTP header
AUTH_PASSWORD. (property name: com.sun.identity.agents.config.iis.password.header)",
          "propertyOrder" : 33730,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : false
            }
          }
        },
        "overrideRequestHost" : {
          "title" : "Override Request URL Host",
          "description" : "Set to true if the agent is sitting behind a ssl/tls
off-loader, load balancer, or proxy to override the host with the value from
the property com.sun.identity.agents.config.agenturi.prefix. (property name:
com.sun.identity.agents.config.override.host)",
          "propertyOrder" : 33200,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : false
            }
          }
        }
      }
    },
    "applicationWebAgentConfig" : {
      "type" : "object",
      "title" : "Application",
      "propertyOrder" : 1,
      "properties" : {
        "responseAttributeFetchMode" : {
          "title" : "Response Attribute Fetch Mode",
```

```
          "description" : "(property name:
 com.sun.identity.agents.config.response.attribute.fetch.mode)",
          "propertyOrder" : 28400,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "notEnforcedIpsRegex" : {
          "title" : "Regular Expressions for Not-Enforced IPs",
          "description" : "Enable use of Perl-compatible regular expressions in Not-Enforced URL from
 IP settings. (property: org.forgerock.agents.config.notenforced.ext.regex.enable)",
          "propertyOrder" : 28150,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : false
            }
          }
        },
        "responseAttributeMap" : {
          "title" : "Response Attribute Map",
          "description" : "Maps the policy response attributes to be populated
 under specific names for the currently authenticated user. (property name:
 com.sun.identity.agents.config.response.attribute.mapping)  <br> Example: <br> To populate the value
 of response attribute uid under name CUSTOM-USER-NAME: enter uid in Map Key field, and enter CUSTOM-
USER-NAME in Corresponding Map Value field.",
          "propertyOrder" : 28500,
          "patternProperties" : {
            ".*" : {
              "type" : "string"
            }
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "object",
              "required" : false
            }
          }
```

```
      },
      "notEnforcedIpsList" : {
        "title" : "Not-Enforced URL from IP Processing List",
        "description" : "Specifies a list of client IP addresses that do not require authentication
when requesting the indicated URLs. <br>The supported format requires a list of IP addresses
separated by spaces, the horizontal bar (|) character, and a list of URLs separated by spaces.
<br>For example: <br>  10.1.2.1 192.168.0.2|/public/* <br>In the preceding example, the IP addresses
10.1.2.1 and  192.168.0.2 can access any resource inside /public without authenticating. (property:
org.forgerock.agents.config.notenforced.ipurl)",
        "propertyOrder" : 28050,
        "items" : {
          "type" : "string"
        },
        "type" : "object",
        "exampleValue" : "",
        "properties" : {
          "inherited" : {
            "type" : "boolean",
            "required" : true
          },
          "value" : {
            "type" : "array",
            "required" : false
          }
        }
      },
      "sessionAttributeMap" : {
        "title" : "Session Attribute Map",
        "description" : "Maps the session attributes to be populated
under specific names for the currently authenticated user. (property name:
com.sun.identity.agents.config.session.attribute.mapping)   <br> Example: <br>  To populate the value
of session attribute UserToken under name CUSTOM-userid: enter UserToken in Map Key field, and enter
CUSTOM-userid in Corresponding Map Value field.",
        "propertyOrder" : 28700,
        "patternProperties" : {
          ".*" : {
            "type" : "string"
          }
        },
        "type" : "object",
        "exampleValue" : "",
        "properties" : {
          "inherited" : {
            "type" : "boolean",
            "required" : true
          },
          "value" : {
            "type" : "object",
            "required" : false
          }
        }
      },
      "fetchAttributesForNotEnforcedUrls" : {
        "title" : "Fetch Attributes for Not Enforced URLs",
        "description" : "Agent fetches profile attributes for not enforced urls by doing policy
evaluation. (property name: com.sun.identity.agents.config.notenforced.url.attributes.enable)",
        "propertyOrder" : 27900,
        "type" : "object",
        "exampleValue" : "",
```

```
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : false
            }
          }
        },
        "notEnforcedUrlsRegex" : {
          "title" : "Regular Expressions for Not-Enforced URLs",
          "description" : "When true, enables use of Perl-compatible regular expressions in Not-
enforced URL settings. (property: com.forgerock.agents.notenforced.url.regex.enable)",
          "propertyOrder" : 27850,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : false
            }
          }
        },
        "ignorePathInfoForNotEnforcedUrls" : {
          "title" : "Ignore Path Info for Not Enforced URLs",
          "description" : "Indicate whether the path info and query should be
 stripped from the request URL before being compared with the URLs of the not
 enforced list when those URLs have a wildcard '*' character.  (property name:
 com.sun.identity.agents.config.ignore.path.info.for.not.enforced.list)  ",
          "propertyOrder" : 27600,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : false
            }
          }
        },
        "sessionAttributeFetchMode" : {
          "title" : "Session Attribute Fetch Mode",
          "description" : "(property name:
 com.sun.identity.agents.config.session.attribute.fetch.mode)",
          "propertyOrder" : 28600,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
```

```
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "clientIpValidation" : {
          "title" : "Client IP Validation",
          "description" : "This validates if the subsequent browser requests come from
the same ip address that the SSO token is initially issued against. (property name:
com.sun.identity.agents.config.client.ip.validation.enable)",
          "propertyOrder" : 28100,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : false
            }
          }
        },
        "profileAttributeFetchMode" : {
          "title" : "Profile Attribute Fetch Mode",
          "description" : "(property name:
com.sun.identity.agents.config.profile.attribute.fetch.mode)",
          "propertyOrder" : 28200,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "invertNotEnforcedUrls" : {
          "title" : "Invert Not Enforced URLs",
          "description" : "Only not enforced list of urls will be enforced. (property name:
com.sun.identity.agents.config.notenforced.url.invert)",
          "propertyOrder" : 27800,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
```

```
              "required" : false
            }
          }
        },
        "notEnforcedUrls" : {
          "title" : "Not Enforced URLs",
          "description" : "List of urls for which no authentication required. (property name:
 com.sun.identity.agents.config.notenforced.url) <br> Example: <br> http://myagent.mydomain.com/
*.gif",
          "propertyOrder" : 27700,
          "items" : {
            "type" : "string"
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "array",
              "required" : false
            }
          }
        },
        "attributeMultiValueSeparator" : {
          "title" : "Attribute Multi Value Separator",
          "description" : "Specifies separator for multiple values. Applies to all
 types of attributes i.e. profile, session and response attributes. (property name:
 com.sun.identity.agents.config.attribute.multi.value.separator)",
          "propertyOrder" : 28800,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "profileAttributeMap" : {
          "title" : "Profile Attribute Map",
          "description" : "Maps the profile attributes to be populated
 under specific names for the currently authenticated user. (property name:
 com.sun.identity.agents.config.profile.attribute.mapping)  <br> Example: <br> To populate the value
 of profile attribute cn under name CUSTOM-Common-Name: enter cn in Map Key field, and enter CUSTOM-
Common-Name in Corresponding Map Value field. <br> To populate the value of profile attribute mail
 under name CUSTOM-Email: enter mail in Map Key field, and enter CUSTOM-Email in Corresponding Map
 Value field.",
          "propertyOrder" : 28300,
          "patternProperties" : {
            ".*" : {
              "type" : "string"
            }
```

```
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "object",
              "required" : false
            }
          }
        },
        "notEnforcedIps" : {
          "title" : "Not Enforced Client IP List",
          "description" : "No authentication and authorization are required for the requests coming
from these client IP addresses. (property name: com.sun.identity.agents.config.notenforced.ip) <br>
Examples: <br> 192.18.145.* <br> 192.18.146.123",
          "propertyOrder" : 28000,
          "items" : {
            "type" : "string"
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "array",
              "required" : false
            }
          }
        },
        "continuousSecurityHeaders" : {
          "title" : "Continuous Security Headers",
          "description" : "The name of the headers in the user's original request, that will be sent
as part of the payload during policy evaluation, which can then be accessed via the 'environment'
variable in a policy script. The 'key' is the name of the header to be sent, and the 'value' is the
name which it will appear as in the policy evaluation script.It is possible to map multiple headers
to the same name (they will simply appear as an array in the evaluation script). If the header
doesn't exist, then the empty string will be sent.",
          "propertyOrder" : 29000,
          "patternProperties" : {
            ".*" : {
              "type" : "string"
            }
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "object",
```

```
              "required" : false
            }
          }
        },
        "continuousSecurityCookies" : {
          "title" : "Continuous Security Cookies",
          "description" : "The name of the cookies to be sent as part of the payload during policy
evaluation, which can be accessed via the 'environment' variable in a policy script. The 'key' is
the name of the cookie to be sent, and the 'value' is the name which it will appear as in the policy
evaluation script. It is possible to map multiple cookies to the same name (they will simply appear
as an array in the evaluation script). If the cookie doesn't exist, then the empty string will be
sent.",
          "propertyOrder" : 28900,
          "patternProperties" : {
            ".*" : {
              "type" : "string"
            }
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "object",
              "required" : false
            }
          }
        }
      }
    }
  }
}
```

delete

Usage:

```
am> delete WebAgents --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action WebAgents --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action WebAgents --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action WebAgents --realm Realm --actionName nextdescendents
```

query

Querying the agents of a specific type

Usage:

```
am> query WebAgents --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read WebAgents --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update WebAgents --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "ssoWebAgentConfig" : {
      "type" : "object",
      "title" : "SSO",
      "propertyOrder" : 2,
      "properties" : {
        "cdssoCookieDomain" : {
          "title" : "Cookies Domain List",
          "description" : "List of domains in which cookies have to be set in CDSSO. (property name:
 com.sun.identity.agents.config.cdsso.cookie.domain) <br> Example: <br> .example.com",
          "propertyOrder" : 29600,
          "items" : {
            "type" : "string"
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "array",
              "required" : false
            }
          }
        },
        "acceptSsoToken" : {
          "title" : "Accept SSO Token",
          "description" : "Specifies whether the agent should accept SSO tokens as session
 cookies alongside with ID tokens. Possible values: <br>- false. The agent does not accept SSO
 Tokens <br>- true. The agent accepts both SSO tokens and ID tokens as session tokens during
 the login flow, and afterwards. SSO tokens are not converted to ID tokens <br>Set this property
 to \"true\" only for specific migration cases (see documentation for more info) <br>(property:
 com.forgerock.agents.accept.sso.token) (Agent 5.7+ only)",
          "propertyOrder" : 29850,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : false
            }
          }
        },
```

```
       "multivaluePreAuthnCookie" : {
         "title" : "Multivalue for Pre-Authn Cookie",
         "description" : "With this set, the agent will use a legacy mode to create cookies that are
used to track unauthenticated requests that have been redirected to login. This mode should only be
used for backward compatibility, where the pre-5.7 way of tracking redirected requests is required,
perhaps because the cookie names are referenced in proxy configuration. This property need not be set
in any other situation. (property: org.forgerock.openam.agents.config.multivalue.pre.authn.cookies)",
         "propertyOrder" : 29280,
         "type" : "object",
         "exampleValue" : "",
         "properties" : {
           "inherited" : {
             "type" : "boolean",
             "required" : true
           },
           "value" : {
             "type" : "boolean",
             "required" : false
           }
         }
       },
       "httpOnly" : {
         "title" : "HTTP Only Mode",
         "description" : "Agents with this property set to true mark cookies as HTTPOnly
to prevent scripts and third-party programs from accessing the cookies. (property:
com.sun.identity.cookie.httponly)",
         "propertyOrder" : 29250,
         "type" : "object",
         "exampleValue" : "",
         "properties" : {
           "inherited" : {
             "type" : "boolean",
             "required" : true
           },
           "value" : {
             "type" : "boolean",
             "required" : false
           }
         }
       },
       "secureCookies" : {
         "title" : "Cookie Security",
         "description" : "Agent sends secure cookies if communication is secure. (property name:
com.sun.identity.agents.config.cookie.secure) <br>Required Agent Restart",
         "propertyOrder" : 29200,
         "type" : "object",
         "exampleValue" : "",
         "properties" : {
           "inherited" : {
             "type" : "boolean",
             "required" : true
           },
           "value" : {
             "type" : "boolean",
             "required" : false
           }
         }
       },
       "cookieResetList" : {
```

```
          "title" : "Cookies Reset Name List",
          "description" : "List of cookies in the format: name[=value][;Domain=value].
(property name: com.sun.identity.agents.config.cookie.reset) <br> Examples: <br> Cookie1 <br>
Cookie2=value;Domain=subdomain.domain.com",
          "propertyOrder" : 29800,
          "items" : {
            "type" : "string"
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "array",
              "required" : false
            }
          }
        },
        "cdssoRedirectUri" : {
          "title" : "CDSSO Redirect URI",
          "description" : "An intermediate URI that is used by the Agent for processing CDSSO
requests. (property name: org.forgerock.agents.authn.redirect.uri) ",
          "propertyOrder" : 29300,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "sameSite" : {
          "title" : "SameSite Cookie Attribute",
          "description" : "If set, agent will add SameSite attribute to all cookies created by
agent with value which is provided in this property. <br>Example: Strict, Lax, None (property:
com.forgerock.agents.cdsso.cookie.samesite)",
          "propertyOrder" : 29260,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "cookieResetOnRedirect" : {
```

```
          "title" : "Session Cookie Reset on Authentication Redirect",
          "description" : "When set to true. the agent will not reset the session cookie on an
authentication redirect if there is a policy advice present.By default, the agent resets the session
cookie in all configured domains on every authentication redirect when a policy advice is present.
(property: org.forgerock.agents.config.cdsso.advice.cleanup.disable)",
          "propertyOrder" : 29400,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : false
            }
          }
        },
        "cookieResetEnabled" : {
          "title" : "Cookie Reset",
          "description" : "Agent resets cookies in the response before redirecting to authentication.
(property name: com.sun.identity.agents.config.cookie.reset.enable)",
          "propertyOrder" : 29700,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : false
            }
          }
        },
        "persistentJwtCookie" : {
          "title" : "Persistent JWT Cookie",
          "description" : "Enable persistence for JWT cookie. If true JWT cookie will not be set as
Session Cookie. (property: org.forgerock.agents.config.cdsso.persistent.cookie.enable)",
          "propertyOrder" : 29270,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : false
            }
          }
        },
        "cookieName" : {
          "title" : "Cookie Name",
          "description" : "Name of the SSO Token cookie used between the AM server and the Agent.
(property name: com.sun.identity.agents.config.cookie.name)<br>Required Agent Restart",
```

```
          "propertyOrder" : 29100,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        }
      }
    },
    "amServicesWebAgent" : {
      "type" : "object",
      "title" : "AM Services",
      "propertyOrder" : 3,
      "properties" : {
        "fetchPoliciesFromRootResource" : {
          "title" : "Fetch Policies from Root Resource",
          "description" : "Agent caches policy decision of the resource and all resources from the
root of the resource down. (property name: com.sun.identity.agents.config.fetch.from.root.resource)
<br>Required Agent Restart",
          "propertyOrder" : 31000,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : false
            }
          }
        },
        "userIdParameterType" : {
          "title" : "User ID Parameter Type",
          "description" : "User ID can be fetched from either SESSION and LDAP attributes. (property
name: com.sun.identity.agents.config.userid.param.type)",
          "propertyOrder" : 30900,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "logoutUrlRegex" : {
```

```
          "title" : "Logout URL Regular Expression",
          "description" : "Perl-compatible regular expression that matches logout URLs. For
 example, to match URLs with protectedA or protectedB in the path and op=logout in the query
 string, use the following setting: <br>*(/protectedA\\?|/protectedB\\?/).*(\\&op=logout\\&)(.*|$)
  <br>When you use this property, the agent ignores the settings for Logout URL List. (property:
 com.forgerock.agents.agent.logout.url.regex)",
          "propertyOrder" : 30540,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "regexConditionalLoginUrl" : {
          "title" : "Regular Expression Conditional Login URL",
          "description" : "Conditionally redirect users based on the incoming request URL. If the
 incoming request URL matches a regular expression, the web agent redirects the request to a specific
 URL. That specific URL can be an AM instance, site, or a different website. Specifies the redirection
 URL and its parameters. This property needs to configure \"Regular Expression Conditional Login
 Pattern\" <br>Example: <br>  org.forgerock.agents.config.conditional.login.pattern[0] = .*shop <br>
  org.forgerock.agents.config.conditional.login.url[0] = http://openam.example.com/openam/oauth2/
authorize?realm=sales <br>(property: org.forgerock.agents.config.conditional.login.url)",
          "propertyOrder" : 30100,
          "items" : {
            "type" : "string"
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "array",
              "required" : false
            }
          }
        },
        "policyCachePollingInterval" : {
          "title" : "Policy Cache Polling Period",
          "description" : "Polling interval in minutes to refresh agent's policy cache. (property
 name: com.sun.identity.agents.config.policy.cache.polling.interval) <br>Required Agent Restart",
          "propertyOrder" : 30600,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
```

```
              "type" : "integer",
              "required" : false
            }
          }
        },
        "amLogoutUrl" : {
          "title" : "AM Logout URL",
          "description" : "AM logout page URL. (property name:
com.sun.identity.agents.config.logout.url)  <br> Example: <br> http://host:port/am/UI/Logout",
          "propertyOrder" : 30200,
          "items" : {
            "type" : "string"
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "array",
              "required" : false
            }
          }
        },
        "userIdParameter" : {
          "title" : "User ID Parameter",
          "description" : "Agent sets value of User Id to REMOTE_USER server variable. (property name:
com.sun.identity.agents.config.userid.param)",
          "propertyOrder" : 30800,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "publicAmUrl" : {
          "title" : "Public AM URL",
          "description" : "Overrides the agent's behavior of finding a suitable AM server and
specifies the public URL of the AM to redirect to. <br> Use this property if: <br>  - Your
environment uses custom login pages (OIDC-compliant and non-OIDC-compliant flows). <br>  - Your
environment's custom login pages are in a network that can only access AM using a proxy, a firewall,
or any other technology that remaps the AM URL to one accessible by the custom login pages. <br>
 -End-users cannot log in due to their cookies being set in the wrong domains. <br>(property:
com.forgerock.agents.public.am.url) ",
          "propertyOrder" : 29950,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
```

```
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "applicationLogoutUrls" : {
          "title" : "Logout URL List",
          "description" : "List of application logout URLs. User gets logged out from AM session
when these urls accessed. (property name: com.sun.identity.agents.config.agent.logout.url). If
this property is used, user should specify a value for the below Logout Redirect URL property. <br>
Example: <br> http://myagent.mydomain.com/logout.html",
          "propertyOrder" : 30300,
          "items" : {
            "type" : "string"
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "array",
              "required" : false
            }
          }
        },
        "logoutRedirectUrl" : {
          "title" : "Logout Redirect URL",
          "description" : "User gets redirected to this url after logout. (property name:
com.sun.identity.agents.config.logout.redirect.url). This property should be specified along with the
above Logout URL List.",
          "propertyOrder" : 30500,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "policyEvaluationRealm" : {
          "title" : "Policy Evaluation Realm",
          "description" : "Which realm to start evaluating from. (property name:
org.forgerock.openam.agents.config.policy.evaluation.realm)",
          "propertyOrder" : 31300,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
```

```
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "retrieveClientHostname" : {
          "title" : "Retrieve Client Hostname",
          "description" : "Gets the client's hostname through DNS reverse lookup for use in policy
evaluation. (property name: com.sun.identity.agents.config.get.client.host.name)",
          "propertyOrder" : 31100,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : false
            }
          }
        },
        "logoutRedirectDisabled" : {
          "title" : "Disabled Logout Redirection",
          "description" : "When disabled, instead of redirecting the user-agent, the web agent
performs session logout in the background and then continues processing access to the current URL.
(property: com.forgerock.agents.config.logout.redirect.disable)",
          "propertyOrder" : 30510,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : false
            }
          }
        },
        "customLoginMode" : {
          "title" : "Custom Login Mode",
          "description" : "Specifies whether the agent should use the default or the custom login
mode when redirecting unauthenticated users.<br>Possible values are: <br>0. Disabled. Default login
redirection mode enabled <br>  1. Custom login mode enabled based on converts the SSO token into an
ID token <br>  2. Legacy Custom login mode. Can be used in specific migration cases from agent 4
<br>(property: org.forgerock.openam.agents.config.allow.custom.login)",
          "propertyOrder" : 29890,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
```

```
              "required" : true
            },
            "value" : {
              "type" : "integer",
              "required" : false
            }
          }
        },
        "logoutResetCookies" : {
          "title" : "Logout Cookies List for Reset",
          "description" : "Any cookies to be reset upon logout in the same format as cookie reset
list. (property name: com.sun.identity.agents.config.logout.cookie.reset) <br> Cookie1 <br>
Cookie2=value;Domain=subdomain.domain.com",
          "propertyOrder" : 30400,
          "items" : {
            "type" : "string"
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "array",
              "required" : false
            }
          }
        },
        "policyEvaluationApplication" : {
          "title" : "Policy Set",
          "description" : "Which application contains the policies to evaluate with. (property name:
org.forgerock.openam.agents.config.policy.evaluation.application)",
          "propertyOrder" : 31400,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "conditionalLoginUrl" : {
          "title" : "AM Conditional Login URL",
          "description" : "Conditionally redirect users based on the incoming request URL. If
the incoming request URL matches a specified domain name, the web agent redirects the request
to a specific URL. That specific URL can be an AM instance, site, or a different website.
<br>Example: <br>  example.com|https://openam.example.com/openam/oauth2/authorize <br>
myapp.domain.com|https://openam2.example.com/openam/oauth2/authorize?realm=sales (property:
com.forgerock.agents.conditional.login.url)",
          "propertyOrder" : 30000,
          "items" : {
            "type" : "string"
```

```
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "array",
              "required" : false
            }
          }
        },
        "regexConditionalLoginPattern" : {
          "title" : "Regular Expression Conditional Login Pattern",
          "description" : "Conditionally redirect users based on the incoming request
 URL. If the incoming request URL matches a regular expression, the web agent redirects
 the request to a specific URL. That specific URL can be an AM instance, site, or
 a different website. Specifies the regular expression that the domain name must
 match. This property needs to configure \"Regular Expression Conditional Login URL\"
 <br>Example: <br>  org.forgerock.agents.config.conditional.login.pattern[0] = .*shop <br>
 org.forgerock.agents.config.conditional.login.url[0] = http://openam.example.com/openam/oauth2/
authorize?realm=sales <br>(property: org.forgerock.agents.config.conditional.login.pattern)",
          "propertyOrder" : 30050,
          "items" : {
            "type" : "string"
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "array",
              "required" : false
            }
          }
        },
        "amLoginUrl" : {
          "title" : "AM Login URL",
          "description" : "AM login page URL. (property name:
 com.sun.identity.agents.config.login.url)  <br> Example: <br> http://host:port/am/UI/Login",
          "propertyOrder" : 29900,
          "items" : {
            "type" : "string"
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "array",
              "required" : false
```

```
            }
          }
        },
        "invalidateLogoutSession" : {
          "title" : "Invalidate Logout Session",
          "description" : "Specifies whether the agent must invalidate the
user session in AM when redirecting to the logout URL specified either by the
Logout URL list (com.sun.identity.agents.config.agent.logout.url) or the AM
logout URL (com.sun.identity.agents.config.logout.url) properties. (property:
org.forgerock.agents.config.logout.session.invalidate)",
          "propertyOrder" : 30520,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : false
            }
          }
        },
        "policyClockSkew" : {
          "title" : "Policy Clock Skew",
          "description" : "Time in seconds used adjust time difference between Agent
machine and AM. Clock skew in seconds = AgentTime - AMServerTime. (property name:
com.sun.identity.agents.config.policy.clock.skew) <br>Required Agent Restart",
          "propertyOrder" : 31200,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "integer",
              "required" : false
            }
          }
        },
        "ssoCachePollingInterval" : {
          "title" : "SSO Cache Polling Period",
          "description" : "Polling interval in minutes to refresh agent's sso cache. (property name:
com.sun.identity.agents.config.sso.cache.polling.interval) <br>Required Agent Restart",
          "propertyOrder" : 30700,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "integer",
              "required" : false
            }
```

```
          }
        },
        "enableLogoutRegex" : {
          "title" : "Enable Regex for Logout URL List",
          "description" : "This property allows regular expressions in \"Logout URL List\" (property:
org.forgerock.agents.config.logout.regex.enable)",
          "propertyOrder" : 30530,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : false
            }
          }
        }
      }
    },
    "globalWebAgentConfig" : {
      "type" : "object",
      "title" : "Global",
      "propertyOrder" : 0,
      "properties" : {
        "status" : {
          "title" : "Status",
          "description" : "Status of the agent configuration.",
          "propertyOrder" : 25100,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : true
            }
          }
        },
        "agentConfigChangeNotificationsEnabled" : {
          "title" : "Agent Configuration Change Notification",
          "description" : "Enable agent to receive notification messages
(via websockets) from AM server for configuration changes. (property name:
org.forgerock.agents.config.change.notifications.enabled) ",
          "propertyOrder" : 25300,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
```

```
              "required" : false
            }
          }
        },
        "jwtName" : {
          "title" : "JWT Cookie Name",
          "description" : "The name used by the agent to set the OIDC JWT on the user's browser.
(property: org.forgerock.agents.jwt.cookie.name)",
          "propertyOrder" : 25500,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "ssoOnlyMode" : {
          "title" : "SSO Only Mode",
          "description" : "Agent will just enforce authentication (SSO), but no authorization for
policies. (property name: com.sun.identity.agents.config.sso.only)",
          "propertyOrder" : 26200,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : false
            }
          }
        },
        "auditLogLocation" : {
          "title" : "Audit Log Location",
          "description" : "Specifies where audit messages should be logged. (property name:
com.sun.identity.agents.config.log.disposition)",
          "propertyOrder" : 26800,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "agentgroup" : {
```

```
          "title" : "Group",
          "description" : "Add the agent to a group to allow inheritance of property values from the
group. <br>Changing the group will update inherited property values. <br>Inherited property values
are copied to the agent.",
          "propertyOrder" : 100,
          "required" : false,
          "type" : "string",
          "exampleValue" : ""
        },
        "fqdnDefault" : {
          "title" : "FQDN Default",
          "description" : "Fully qualified hostname that the users should use in order to access
resources. (property name: com.sun.identity.agents.config.fqdn.default)",
          "propertyOrder" : 27400,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "resetIdleTime" : {
          "title" : "Reset Idle Timeout",
          "description" : "If the agent is configured in SSO-only mode, the session may unexpectedly
expire in AM due to idle timeout before the user has finished accessing the application. <br>Set
this property to true to refresh the timeout when the user performs an action. <br>When set to
true, the agent makes an additional call to AM, this may cause a performance impact. Configure this
property only if: <br>   The agent is configured in SSO-only mode. <br>   User's sessions are timing
out in AM because they are unexpectedly reaching the maximum idle timeout value. <br>(property:
com.forgerock.agents.call.session.refresh)",
          "propertyOrder" : 26250,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : false
            }
          }
        },
        "agentDebugLevel" : {
          "title" : "Agent Debug Level",
          "description" : "Agent debug level. (property name:
com.sun.identity.agents.config.debug.level)",
          "propertyOrder" : 26400,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
```

```
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "userpassword" : {
          "title" : "Password",
          "description" : "",
          "propertyOrder" : 25000,
          "required" : true,
          "type" : "string",
          "format" : "password",
          "exampleValue" : ""
        },
        "accessDeniedUrl" : {
          "title" : "Resources Access Denied URL",
          "description" : "The URL of the customized access denied page. (property name:
com.sun.identity.agents.config.access.denied.url)",
          "propertyOrder" : 26300,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "auditAccessType" : {
          "title" : "Audit Access Types",
          "description" : "Types of messages to log based on user URL access attempts. (property name:
com.sun.identity.agents.config.audit.accesstype)",
          "propertyOrder" : 26700,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "notificationsEnabled" : {
          "title" : "Enable Notifications",
          "description" : "The notifications help in maintaining agent's sso, policy and configuration
caches. (property name: com.sun.identity.agents.config.notification.enable) <br>Required Agent
Restart",
```

```
          "propertyOrder" : 25600,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : false
            }
          }
        },
        "fqdnMapping" : {
          "title" : "FQDN Virtual Host Map",
          "description" : "Maps virtual, invalid, or partial hostnames, and IP addresses to the FQDN
to access protected resources. (property name: com.sun.identity.agents.config.fqdn.mapping) <br>
Examples: <br>  To map the partial hostname myserver to myserver.mydomain.com: enter myserver in the
Map Key field and myserver.mydomain.com in the Corresponding Map Value field. To map a virtual server
rst.hostname.com that points to the actual server abc.hostname.com: enter valid1 in the Map Key field
and rst.hostname.com in the Corresponding Map Value field.",
          "propertyOrder" : 27500,
          "patternProperties" : {
            ".*" : {
              "type" : "string"
            }
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "object",
              "required" : false
            }
          }
        },
        "configurationPollingInterval" : {
          "title" : "Configuration Reload Interval",
          "description" : "Interval in minutes to fetch agent configuration from AM. (property name:
com.sun.identity.agents.config.polling.interval) <br>Required Agent Restart",
          "propertyOrder" : 25900,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "integer",
              "required" : false
            }
          }
        },
```

```
       "cdssoRootUrl" : {
         "title" : "Agent Root URL for CDSSO",
         "description" : "The agent root URL for CDSSO. The valid value is in the following format:
<br>protocol://hostname:port/<br> The protocol represents the protocol used, such as http or https.
The hostname represents the host name of the machine on which the agent resides. The port represents
the port number on which the agent is installed. The slash following the port number is required.",
         "propertyOrder" : 26100,
         "items" : {
           "type" : "string"
         },
         "type" : "object",
         "exampleValue" : "",
         "properties" : {
           "inherited" : {
             "type" : "boolean",
             "required" : true
           },
           "value" : {
             "type" : "array",
             "required" : false
           }
         }
       },
       "fqdnCheck" : {
         "title" : "FQDN Check",
         "description" : "Enables checking of fqdn default value and fqdn map values. (property name:
com.sun.identity.agents.config.fqdn.check.enable)",
         "propertyOrder" : 27300,
         "type" : "object",
         "exampleValue" : "",
         "properties" : {
           "inherited" : {
             "type" : "boolean",
             "required" : true
           },
           "value" : {
             "type" : "boolean",
             "required" : false
           }
         }
       },
       "jwtAuditWhitelist" : {
         "title" : "Agent Profile ID Whitelist",
         "description" : "Specifies a comma-separated list of profile IDs that the agent will
consider as valid values for the aud claim. This claim is represented in the JWT containing
the end user's session. <br>Example: <br>agentprofile1,agentprofile2,.... <br>When several
agents configured with different agent profiles protect the same application, set this property
to a list of the agent profiles that are protecting the same application. <br>(property:
com.forgerock.agents.jwt.aud.whitelist)",
         "propertyOrder" : 25520,
         "type" : "object",
         "exampleValue" : "",
         "properties" : {
           "inherited" : {
             "type" : "boolean",
             "required" : true
           },
           "value" : {
             "type" : "string",
```

```
              "required" : false
            }
          }
        },
        "webSocketConnectionIntervalInMinutes" : {
          "title" : "Web Socket Connection Interval",
          "description" : "Interval in minutes by which agents reopen their web socket
connection to ensure a fair distribution of connections across AM servers. (property:
org.forgerock.agents.balance.websocket.interval.minutes).",
          "propertyOrder" : 25400,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "integer",
              "required" : false
            }
          }
        },
        "disableJwtAudit" : {
          "title" : "Disable validation of the audience claim",
          "description" : "Specifies whether the agent should validate the audience claim matches the
agent profile ID represented in the JWT containing the end user's session. <br>Possible values are:
<br>  false = The agent validates audience claim. <br>  true = The agent does not validate audience
claim.<br> (property: com.forgerock.agents.jwt.aud.disable)",
          "propertyOrder" : 25510,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : false
            }
          }
        },
        "agentUriPrefix" : {
          "title" : "Agent Deployment URI Prefix",
          "description" : "(property name: com.sun.identity.agents.config.agenturi.prefix)",
          "propertyOrder" : 25800,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
```

```
       },
       "repositoryLocation" : {
         "title" : "Location of Agent Configuration Repository",
         "description" : "Indicates agent's configuration located either on agent's host or centrally
on AM server (property: org.forgerock.agents.config.location).",
         "propertyOrder" : 25200,
         "required" : true,
         "type" : "string",
         "exampleValue" : ""
       }
     }
   },
   "miscWebAgentConfig" : {
     "type" : "object",
     "title" : "Miscellaneous",
     "propertyOrder" : 4,
     "properties" : {
       "ignorePathInfo" : {
         "title" : "Ignore Path Info in Request URL",
         "description" : "The path info will be stripped from the request URL while doing Not
Enforced List check and url policy evaluation if the value is set to true. (property name:
com.sun.identity.agents.config.ignore.path.info)",
         "propertyOrder" : 32400,
         "type" : "object",
         "exampleValue" : "",
         "properties" : {
           "inherited" : {
             "type" : "boolean",
             "required" : true
           },
           "value" : {
             "type" : "boolean",
             "required" : false
           }
         }
       },
       "invalidUrlRegex" : {
         "title" : "Invalid URL Regular Expression",
         "description" : "Specifies a Perl-compatible regular expression to parse valid request
URLs. The web agent rejects requests to invalid URLs with HTTP 403 Forbidden status without
further processing. <br>Example, to filter out URLs containing a list of characters and words
such as ./ /. / . %00-%1f, %7f-%ff, %25, %2B, %2C, %7E, .info, configure the following regular
expression: <br>^(\\?!.\\/|\\/.|.|.info|%2B|%00-%1f|%7f-%ff|%25|%2C|%7E).*$ <br>(property:
com.forgerock.agents.agent.invalid.url.regex)",
         "propertyOrder" : 32500,
         "type" : "object",
         "exampleValue" : "",
         "properties" : {
           "inherited" : {
             "type" : "boolean",
             "required" : true
           },
           "value" : {
             "type" : "string",
             "required" : false
           }
         }
       },
       "encodeUrlSpecialCharacters" : {
```

```
          "title" : "Encode URL's Special Characters",
          "description" : "Encodes the url which has special characters before doing policy
evaluation. (property name: com.sun.identity.agents.config.encode.url.special.chars.enable)",
          "propertyOrder" : 32100,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : false
            }
          }
        },
        "profileAttributesCookiePrefix" : {
          "title" : "Profile Attributes Cookie Prefix",
          "description" : "Sets cookie prefix in the attributes headers. (property name:
com.sun.identity.agents.config.profile.attribute.cookie.prefix)",
          "propertyOrder" : 31800,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "headerJsonResponse" : {
          "title" : "Headers and Values to Receive JSON-Formatted Responses",
          "description" : "Specify HTTP headers and associated values
that trigger JSON-formatted errors to be returned. <br>Example:
<br>org.forgerock.agents.config.json.header[enableJsonResponse]=true
<br>org.forgerock.agents.config.json.response.code=202 <br>(property:
org.forgerock.agents.config.json.header[Header]=Value)",
          "propertyOrder" : 32740,
          "patternProperties" : {
            ".*" : {
              "type" : "string"
            }
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "object",
              "required" : false
            }
```

```
        }
      },
      "anonymousUserId" : {
        "title" : "Anonymous User Default Value",
        "description" : "User id of unauthenticated users. (property name:
com.sun.identity.agents.config.anonymous.user.id)",
        "propertyOrder" : 32700,
        "type" : "object",
        "exampleValue" : "",
        "properties" : {
          "inherited" : {
            "type" : "boolean",
            "required" : true
          },
          "value" : {
            "type" : "string",
            "required" : false
          }
        }
      },
      "invertUrlJsonResponse" : {
        "title" : "Invert Properties That Receive JSON-Formatted Responses",
        "description" : "Set to true to invert the meaning of both the
org.forgerock.agents.config.json.url and org.forgerock.agents.config.json.header properties.
When inverted the specified values in those two properties will not trigger JSON-formatted
responses. Any non-specified value will trigger JSON-formatted responses, instead. (property:
org.forgerock.agents.config.json.url.invert)",
        "propertyOrder" : 32750,
        "type" : "object",
        "exampleValue" : "",
        "properties" : {
          "inherited" : {
            "type" : "boolean",
            "required" : true
          },
          "value" : {
            "type" : "boolean",
            "required" : false
          }
        }
      },
      "profileAttributesCookieMaxAge" : {
        "title" : "Profile Attributes Cookie Maxage",
        "description" : "Maxage of attributes cookie headers. (property name:
com.sun.identity.agents.config.profile.attribute.cookie.maxage)",
        "propertyOrder" : 31900,
        "type" : "object",
        "exampleValue" : "",
        "properties" : {
          "inherited" : {
            "type" : "boolean",
            "required" : true
          },
          "value" : {
            "type" : "integer",
            "required" : false
          }
        }
      },
```

```
       "anonymousUserEnabled" : {
         "title" : "Anonymous User",
         "description" : "Enable/Disable REMOTE_USER processing for anonymous users. (property name:
com.sun.identity.agents.config.anonymous.user.enable)",
         "propertyOrder" : 31600,
         "type" : "object",
         "exampleValue" : "",
         "properties" : {
           "inherited" : {
             "type" : "boolean",
             "required" : true
           },
           "value" : {
             "type" : "boolean",
             "required" : false
           }
         }
       },
       "mineEncodeHeader" : {
         "title" : "MIME-Encode HTTP Header Values",
         "description" : "Specifies whether the agent must MIME-encode HTTP header values, and
when to do it. Possible values are: <br>  0. The agent MIME-encodes the value of HTTP headers
if said value is a multi-byte Unicode string. <br>  1. The agent MIME-encodes the value of every
HTTP header. <br>  2. The agent does not MIME-encode the value of any HTTP header. <br> (property:
com.forgerock.agents.header.mime.encode)",
         "propertyOrder" : 32720,
         "type" : "object",
         "exampleValue" : "",
         "properties" : {
           "inherited" : {
             "type" : "boolean",
             "required" : true
           },
           "value" : {
             "type" : "integer",
             "required" : false
           }
         }
       },
       "compositeAdviceEncode" : {
         "title" : "Composite Advice Encode",
         "description" : "This property is used to specify whether AM composite advices
should be based64url encoded before sending to custom login endpoints. (property:
com.forgerock.agents.advice.b64.url.encode)",
         "propertyOrder" : 32300,
         "type" : "object",
         "exampleValue" : "",
         "properties" : {
           "inherited" : {
             "type" : "boolean",
             "required" : true
           },
           "value" : {
             "type" : "boolean",
             "required" : false
           }
         }
       },
       "addCacheControlHeader" : {
```

```
          "title" : "Add Cache-Control Headers",
          "description" : "Set this property to true to enable use of Cache-Control headers
 that prevent proxies from caching resources accessed by unauthenticated users. (property:
 com.forgerock.agents.cache_control_header.enable)",
          "propertyOrder" : 32710,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : false
            }
          }
        },
        "statusCodeJsonResponse" : {
          "title" : "HTTP Return Code for JSON-Formatted Responses",
          "description" : "Specifies an HTTP response code to return when a JSON-formatted error is
 triggered. (property: org.forgerock.agents.config.json.response.code)",
          "propertyOrder" : 32760,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "integer",
              "required" : false
            }
          }
        },
        "gotoParameterName" : {
          "title" : "Goto Parameter Name",
          "description" : "This is the name of the HTTP query \"goto\" parameter. It is not
 recommended to change it. (property name: com.sun.identity.agents.config.redirect.param) ",
          "propertyOrder" : 32600,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "urlJsonResponse" : {
          "title" : "URLs to Receive JSON-Formatted Responses",
          "description" : "Returning the responses in JSON format is useful for non-
browser-based, or AJAX applications, that may not want to redirect users to the AM user
 interface for authentication. <br>Example: org.forgerock.agents.config.json.url[0]=http*://
```

```
*.example.com:*/api/* <br>org.forgerock.agents.config.json.response.code=202 <br>(property:
 org.forgerock.agents.config.json.url)",
          "propertyOrder" : 32730,
          "items" : {
            "type" : "string"
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "array",
              "required" : false
            }
          }
        },
        "encodeSpecialCharsInCookies" : {
          "title" : "Encode special chars in Cookies",
          "description" : "Encode special chars in cookie by URL encoding. Useful when profile,
 session and response attributes contain special chars and attributes fetch mode is set to
 HTTP_COOKIE. (property name: com.sun.identity.agents.config.encode.cookie.special.chars.enable)  ",
          "propertyOrder" : 31700,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : false
            }
          }
        },
        "caseInsensitiveUrlComparison" : {
          "title" : "URL Comparison Case Sensitivity Check",
          "description" : "Enforces case insensitivity in both policy and not enforced url evaluation.
 (property name: com.sun.identity.agents.config.url.comparison.case.ignore)",
          "propertyOrder" : 32000,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : false
            }
          }
        },
        "compositeAdviceRedirect" : {
          "title" : "Composite Advice Handling",
```

```
          "description" : "When set to true, the agent sends composite advice in
the query (GET request) instead of sending it through a POST request. (property:
com.sun.am.use_redirect_for_advice)",
          "propertyOrder" : 32200,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : false
            }
          }
        }
      }
    },
    "advancedWebAgentConfig" : {
      "type" : "object",
      "title" : "Advanced",
      "propertyOrder" : 5,
      "properties" : {
        "showPasswordInHeader" : {
          "title" : "Show Password in HTTP Header",
          "description" : "Set to true if encrypted password should be set in HTTP header
AUTH_PASSWORD. (property name: com.sun.identity.agents.config.iis.password.header)",
          "propertyOrder" : 34400,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : false
            }
          }
        },
        "logonAndImpersonation" : {
          "title" : "Logon and Impersonation",
          "description" : "Set to true if agent should do Windows Logon and User Impersonation.
(property name: com.sun.identity.agents.config.iis.logonuser)",
          "propertyOrder" : 34500,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : false
            }
          }
```

```
        },
        "pdpStickySessionCookieName" : {
          "title" : "POST Data Sticky Load Balancing Cookie Name",
          "description" : "Specifies the name of a cookie to use for enabling sticky load balancing
 when the \"POST Data Sticky Load Balancing Mode\" property is set to COOKIE. Set the cookie name
 to the same value configured in the \"POST Data Sticky Load Balancing Value\" property. (property:
 com.sun.identity.agents.config.postdata.preserve.lbcookie)",
          "propertyOrder" : 33720,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "pdpSkipPostUrl" : {
          "title" : "URLs Ignored by the Agent POST Data Inspector",
          "description" : "Specifies a list of URLs that will not be processed by the web agent
 POST data inspector. This allows other modules on the same server to access the POST data directly.
 <br>The following example uses wildcards to add a file named postreader.jsp in the root of any
 protected website to the list of URLs that will not have their POST data inspected: <br>http*://*:*/
postreader.jsp <br>Any URLs added to this property should also be added to the Not-Enforced URLs <br>
 (property: org.forgerock.agents.config.skip.post.url)",
          "propertyOrder" : 33740,
          "items" : {
            "type" : "string"
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "array",
              "required" : false
            }
          }
        },
        "postDataPreservation" : {
          "title" : "POST Data Preservation",
          "description" : "Enables POST data preservation. (property name:
 com.sun.identity.agents.config.postdata.preserve.enable) <br> Note that this feature is not supported
 in all the web agents. Please refer individual agents documentation for more details.",
          "propertyOrder" : 33500,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
```

```
            "value" : {
              "type" : "boolean",
              "required" : false
            }
          }
        },
        "overrideRequestProtocol" : {
          "title" : "Override Request URL Protocol",
          "description" : "Set to true if the agent is sitting behind a ssl/tls
off-loader, load balancer, or proxy to override the protocol with the value from
the property com.sun.identity.agents.config.agenturi.prefix. (property name:
com.sun.identity.agents.config.override.protocol)",
          "propertyOrder" : 33100,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : false
            }
          }
        },
        "customProperties" : {
          "title" : "Custom Properties",
          "description" : "Additional properties that allow users to augment the set of
properties supported by agent. (property name: com.sun.identity.agents.config.freeformproperties)
 <br> Examples: <br> customproperty=custom-value1 <br> customlist[0]=customlist-value-0
<br> customlist[1]=customlist-value-1 <br> custommap[key1]=custommap-value-1 <br>
custommap[key2]=custommap-value-2",
          "propertyOrder" : 35100,
          "items" : {
            "type" : "string"
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "array",
              "required" : false
            }
          }
        },
        "pdpStickySessionMode" : {
          "title" : "POST Data Sticky Load Balancing Mode",
          "description" : "Specifies whether to create a cookie, or to append a
query string to the URL to assist with sticky load balancing. Possible values
are: <br>COOKIE. The web agent creates a cookie with the value specified
in the com.sun.identity.agents.config.postdata.preserve.stickysession.value
property. <br>URL. The web agent appends the value specified in the
com.sun.identity.agents.config.postdata.preserve.stickysession.value to the URL query string. <br>
(property: com.sun.identity.agents.config.postdata.preserve.stickysession.mode)",
```

```
          "propertyOrder" : 33700,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "fragmentRedirectEnabled" : {
          "title" : "Fragment Redirect Enabled",
          "description" : "Enable to save the browser's URL fragment during authentication.
<br>(property: org.forgerock.agents.config.fragment.redirect.enable) (Agent 5.7+ only)",
          "propertyOrder" : 33400,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : false
            }
          }
        },
        "overrideRequestPort" : {
          "title" : "Override Request URL Port",
          "description" : "Set to true if the agent is sitting behind a ssl/tls
off-loader, load balancer, or proxy to override the port with the value from
the property com.sun.identity.agents.config.agenturi.prefix. (property name:
com.sun.identity.agents.config.override.port)",
          "propertyOrder" : 33300,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : false
            }
          }
        },
        "postDataCachePeriod" : {
          "title" : "POST Data Entries Cache Period",
          "description" : "POST cache entry lifetime in minutes. (property name:
com.sun.identity.agents.config.postcache.entry.lifetime)",
          "propertyOrder" : 33600,
          "type" : "object",
          "exampleValue" : "",
```

```
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "integer",
              "required" : false
            }
          }
        },
        "pdpStickySessionValue" : {
          "title" : "POST Data Sticky Load Balancing Value",
          "description" : "Specifies a key-value pair separated by the = character that the web
agent creates when evaluating the \"POST Data Sticky Load Balancing Mode\". For example, a setting
of lb=myserver either sets an lb cookie with myserver value, or adds lb=myserver to the URL query
string. When configuring POST data preservation with cookies, set the cookie name in the cookie
pair to the same value configured in the \"POST Data Sticky Load Balancing Cookie Name\". (property:
com.sun.identity.agents.config.postdata.preserve.stickysession.value)",
          "propertyOrder" : 33710,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "replayPasswordKey" : {
          "title" : "Replay Password Key",
          "description" : "DES key for decrypting the basic authentication password in the session.
(property name: com.sun.identity.agents.config.replaypasswd.key)",
          "propertyOrder" : 33900,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "clientIpHeader" : {
          "title" : "Client IP Address Header",
          "description" : "HTTP header name that holds the IP address of the client. (property name:
org.forgerock.agents.http.header.containing.ip.address) ",
          "propertyOrder" : 32800,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
```

```
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "clientHostnameHeader" : {
          "title" : "Client Hostname Header",
          "description" : "HTTP header name that holds the Hostname of the client. (property name:
org.forgerock.agents.http.header.containing.remote.hostname) ",
          "propertyOrder" : 32900,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "pdpJavascriptRepost" : {
          "title" : "Show Password in HTTP Header",
          "description" : "Set to true if encrypted password should be set in HTTP header
AUTH_PASSWORD. (property name: com.sun.identity.agents.config.iis.password.header)",
          "propertyOrder" : 33730,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : false
            }
          }
        },
        "overrideRequestHost" : {
          "title" : "Override Request URL Host",
          "description" : "Set to true if the agent is sitting behind a ssl/tls
off-loader, load balancer, or proxy to override the host with the value from
the property com.sun.identity.agents.config.agenturi.prefix. (property name:
com.sun.identity.agents.config.override.host)",
          "propertyOrder" : 33200,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
```

```
            },
            "value" : {
              "type" : "boolean",
              "required" : false
            }
          }
        }
      }
    },
    "applicationWebAgentConfig" : {
      "type" : "object",
      "title" : "Application",
      "propertyOrder" : 1,
      "properties" : {
        "responseAttributeFetchMode" : {
          "title" : "Response Attribute Fetch Mode",
          "description" : "(property name:
 com.sun.identity.agents.config.response.attribute.fetch.mode)",
          "propertyOrder" : 28400,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "notEnforcedIpsRegex" : {
          "title" : "Regular Expressions for Not-Enforced IPs",
          "description" : "Enable use of Perl-compatible regular expressions in Not-Enforced URL from
 IP settings. (property: org.forgerock.agents.config.notenforced.ext.regex.enable)",
          "propertyOrder" : 28150,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : false
            }
          }
        },
        "responseAttributeMap" : {
          "title" : "Response Attribute Map",
          "description" : "Maps the policy response attributes to be populated
 under specific names for the currently authenticated user. (property name:
 com.sun.identity.agents.config.response.attribute.mapping)  <br> Example: <br> To populate the value
 of response attribute uid under name CUSTOM-USER-NAME: enter uid in Map Key field, and enter CUSTOM-
USER-NAME in Corresponding Map Value field.",
          "propertyOrder" : 28500,
          "patternProperties" : {
```

```
            ".*" : {
              "type" : "string"
            }
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "object",
              "required" : false
            }
          }
        },
        "notEnforcedIpsList" : {
          "title" : "Not-Enforced URL from IP Processing List",
          "description" : "Specifies a list of client IP addresses that do not require authentication
when requesting the indicated URLs. <br>The supported format requires a list of IP addresses
separated by spaces, the horizontal bar (|) character, and a list of URLs separated by spaces.
<br>For example: <br>  10.1.2.1 192.168.0.2|/public/* <br>In the preceding example, the IP addresses
10.1.2.1 and  192.168.0.2 can access any resource inside /public without authenticating. (property:
org.forgerock.agents.config.notenforced.ipurl)",
          "propertyOrder" : 28050,
          "items" : {
            "type" : "string"
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "array",
              "required" : false
            }
          }
        },
        "sessionAttributeMap" : {
          "title" : "Session Attribute Map",
          "description" : "Maps the session attributes to be populated
under specific names for the currently authenticated user. (property name:
com.sun.identity.agents.config.session.attribute.mapping)   <br> Example: <br>  To populate the value
of session attribute UserToken under name CUSTOM-userid: enter UserToken in Map Key field, and enter
CUSTOM-userid in Corresponding Map Value field.",
          "propertyOrder" : 28700,
          "patternProperties" : {
            ".*" : {
              "type" : "string"
            }
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
```

```
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "object",
              "required" : false
            }
          }
        },
        "fetchAttributesForNotEnforcedUrls" : {
          "title" : "Fetch Attributes for Not Enforced URLs",
          "description" : "Agent fetches profile attributes for not enforced urls by doing policy
 evaluation. (property name: com.sun.identity.agents.config.notenforced.url.attributes.enable)",
          "propertyOrder" : 27900,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : false
            }
          }
        },
        "notEnforcedUrlsRegex" : {
          "title" : "Regular Expressions for Not-Enforced URLs",
          "description" : "When true, enables use of Perl-compatible regular expressions in Not-
enforced URL settings. (property: com.forgerock.agents.notenforced.url.regex.enable)",
          "propertyOrder" : 27850,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : false
            }
          }
        },
        "ignorePathInfoForNotEnforcedUrls" : {
          "title" : "Ignore Path Info for Not Enforced URLs",
          "description" : "Indicate whether the path info and query should be
 stripped from the request URL before being compared with the URLs of the not
 enforced list when those URLs have a wildcard '*' character.  (property name:
 com.sun.identity.agents.config.ignore.path.info.for.not.enforced.list)  ",
          "propertyOrder" : 27600,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
```

```
            "value" : {
              "type" : "boolean",
              "required" : false
            }
          }
        },
        "sessionAttributeFetchMode" : {
          "title" : "Session Attribute Fetch Mode",
          "description" : "(property name:
com.sun.identity.agents.config.session.attribute.fetch.mode)",
          "propertyOrder" : 28600,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
          }
        },
        "clientIpValidation" : {
          "title" : "Client IP Validation",
          "description" : "This validates if the subsequent browser requests come from
the same ip address that the SSO token is initially issued against. (property name:
com.sun.identity.agents.config.client.ip.validation.enable)",
          "propertyOrder" : 28100,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : false
            }
          }
        },
        "profileAttributeFetchMode" : {
          "title" : "Profile Attribute Fetch Mode",
          "description" : "(property name:
com.sun.identity.agents.config.profile.attribute.fetch.mode)",
          "propertyOrder" : 28200,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
```

```
          }
        },
        "invertNotEnforcedUrls" : {
          "title" : "Invert Not Enforced URLs",
          "description" : "Only not enforced list of urls will be enforced. (property name:
 com.sun.identity.agents.config.notenforced.url.invert)",
          "propertyOrder" : 27800,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "boolean",
              "required" : false
            }
          }
        },
        "notEnforcedUrls" : {
          "title" : "Not Enforced URLs",
          "description" : "List of urls for which no authentication required. (property name:
 com.sun.identity.agents.config.notenforced.url) <br> Example: <br> http://myagent.mydomain.com/
*.gif",
          "propertyOrder" : 27700,
          "items" : {
            "type" : "string"
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "array",
              "required" : false
            }
          }
        },
        "attributeMultiValueSeparator" : {
          "title" : "Attribute Multi Value Separator",
          "description" : "Specifies separator for multiple values. Applies to all
 types of attributes i.e. profile, session and response attributes. (property name:
 com.sun.identity.agents.config.attribute.multi.value.separator)",
          "propertyOrder" : 28800,
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "string",
              "required" : false
            }
```

```
          }
        },
        "profileAttributeMap" : {
          "title" : "Profile Attribute Map",
          "description" : "Maps the profile attributes to be populated
 under specific names for the currently authenticated user. (property name:
 com.sun.identity.agents.config.profile.attribute.mapping)  <br> Example: <br> To populate the value
 of profile attribute cn under name CUSTOM-Common-Name: enter cn in Map Key field, and enter CUSTOM-
Common-Name in Corresponding Map Value field. <br> To populate the value of profile attribute mail
 under name CUSTOM-Email: enter mail in Map Key field, and enter CUSTOM-Email in Corresponding Map
 Value field.",
          "propertyOrder" : 28300,
          "patternProperties" : {
            ".*" : {
              "type" : "string"
            }
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "object",
              "required" : false
            }
          }
        },
        "notEnforcedIps" : {
          "title" : "Not Enforced Client IP List",
          "description" : "No authentication and authorization are required for the requests coming
 from these client IP addresses. (property name: com.sun.identity.agents.config.notenforced.ip) <br>
 Examples: <br> 192.18.145.* <br> 192.18.146.123",
          "propertyOrder" : 28000,
          "items" : {
            "type" : "string"
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "array",
              "required" : false
            }
          }
        },
        "continuousSecurityHeaders" : {
          "title" : "Continuous Security Headers",
          "description" : "The name of the headers in the user's original request, that will be sent
 as part of the payload during policy evaluation, which can then be accessed via the 'environment'
 variable in a policy script. The 'key' is the name of the header to be sent, and the 'value' is the
 name which it will appear as in the policy evaluation script.It is possible to map multiple headers
```

```
 to the same name (they will simply appear as an array in the evaluation script). If the header
 doesn't exist, then the empty string will be sent.",
          "propertyOrder" : 29000,
          "patternProperties" : {
            ".*" : {
              "type" : "string"
            }
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "object",
              "required" : false
            }
          }
        },
        "continuousSecurityCookies" : {
          "title" : "Continuous Security Cookies",
          "description" : "The name of the cookies to be sent as part of the payload during policy
 evaluation, which can be accessed via the 'environment' variable in a policy script. The 'key' is
 the name of the cookie to be sent, and the 'value' is the name which it will appear as in the policy
 evaluation script. It is possible to map multiple cookies to the same name (they will simply appear
 as an array in the evaluation script). If the cookie doesn't exist, then the empty string will be
 sent.",
          "propertyOrder" : 28900,
          "patternProperties" : {
            ".*" : {
              "type" : "string"
            }
          },
          "type" : "object",
          "exampleValue" : "",
          "properties" : {
            "inherited" : {
              "type" : "boolean",
              "required" : true
            },
            "value" : {
              "type" : "object",
              "required" : false
            }
          }
        }
      }
    }
  }
}
```

WebAuthnAuthenticationNode

Realm Operations

Resource path: `/realm-config/authentication/authenticationtrees/nodes/WebAuthnAuthenticationNode`

Resource version: `1.0`

create

Usage:

```
am> create WebAuthnAuthenticationNode --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "isRecoveryCodeAllowed" : {
      "title" : "Allow recovery codes",
      "description" : "",
      "propertyOrder" : 30,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "asScript" : {
      "title" : "Return challenge as JavaScript",
      "description" : "If enabled, the node will return its challenge as a fully encapsulated client-
side JavaScript that will interact directly with the WebAuthn API and submit the response back. If
 disabled, the node will return the challenge and associated data in a metadata node, and the custom
 UI will use that to interact with the WebAuthn API itself.",
      "propertyOrder" : 60,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "relyingPartyDomain" : {
      "title" : "Relying party identifier",
      "description" : "The domain against which to register devices, if blank AM will make a best
 guess at the domain.",
      "propertyOrder" : 10,
```

```
      "type" : "string",
      "exampleValue" : ""
    },
    "requiresResidentKey" : {
      "title" : "Username from device",
      "description" : "Requests that the username is selected by the device. Devices which do not
 support storing and providing the username will be unable to utilise the node while it is operating
 in this mode.",
      "propertyOrder" : 50,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "origins" : {
      "title" : "Origin domains",
      "description" : "A set of fully-qualified URLs of accepted origins, e.g. http://
app.example.com:443. If empty, the accepted origin is the incoming request origin.",
      "propertyOrder" : 15,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "userVerificationRequirement" : {
      "title" : "User verification requirement",
      "description" : "If specified as REQUIRED, authenticators that don't verify user identity are
 filtered out and should not be selectable by the user.",
      "propertyOrder" : 20,
      "type" : "string",
      "exampleValue" : ""
    },
    "timeout" : {
      "title" : "Timeout",
      "description" : "The number of seconds to wait for a valid WebAuthn authenticator to be
 registered before failing.",
      "propertyOrder" : 40,
      "type" : "integer",
      "exampleValue" : ""
    }
  },
  "required" : [ "asScript", "origins", "timeout", "requiresResidentKey", "isRecoveryCodeAllowed",
 "userVerificationRequirement" ]
}
```


delete

Usage:

```
am> delete WebAuthnAuthenticationNode --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action WebAuthnAuthenticationNode --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action WebAuthnAuthenticationNode --realm Realm --actionName getCreatableTypes
```

listOutcomes

List the available outcomes for the node type.

Usage:

```
am> action WebAuthnAuthenticationNode --realm Realm --body body --actionName listOutcomes
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "title" : "Some configuration of the node. This does not need to be complete against the
 configuration schema."
}
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action WebAuthnAuthenticationNode --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query WebAuthnAuthenticationNode --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read WebAuthnAuthenticationNode --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update WebAuthnAuthenticationNode --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "isRecoveryCodeAllowed" : {
      "title" : "Allow recovery codes",
      "description" : "",
      "propertyOrder" : 30,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "asScript" : {
      "title" : "Return challenge as JavaScript",
      "description" : "If enabled, the node will return its challenge as a fully encapsulated client-
side JavaScript that will interact directly with the WebAuthn API and submit the response back. If
 disabled, the node will return the challenge and associated data in a metadata node, and the custom
 UI will use that to interact with the WebAuthn API itself.",
      "propertyOrder" : 60,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "relyingPartyDomain" : {
```

```
      "title" : "Relying party identifier",
      "description" : "The domain against which to register devices, if blank AM will make a best
 guess at the domain.",
      "propertyOrder" : 10,
      "type" : "string",
      "exampleValue" : ""
    },
    "requiresResidentKey" : {
      "title" : "Username from device",
      "description" : "Requests that the username is selected by the device. Devices which do not
 support storing and providing the username will be unable to utilise the node while it is operating
 in this mode.",
      "propertyOrder" : 50,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "origins" : {
      "title" : "Origin domains",
      "description" : "A set of fully-qualified URLs of accepted origins, e.g. http://
app.example.com:443. If empty, the accepted origin is the incoming request origin.",
      "propertyOrder" : 15,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "userVerificationRequirement" : {
      "title" : "User verification requirement",
      "description" : "If specified as REQUIRED, authenticators that don't verify user identity are
 filtered out and should not be selectable by the user.",
      "propertyOrder" : 20,
      "type" : "string",
      "exampleValue" : ""
    },
    "timeout" : {
      "title" : "Timeout",
      "description" : "The number of seconds to wait for a valid WebAuthn authenticator to be
 registered before failing.",
      "propertyOrder" : 40,
      "type" : "integer",
      "exampleValue" : ""
    }
  },
  "required" : [ "asScript", "origins", "timeout", "requiresResidentKey", "isRecoveryCodeAllowed",
 "userVerificationRequirement" ]
}
```


WebAuthnDeviceStorageNode

Realm Operations

Resource path: `/realm-config/authentication/authenticationtrees/nodes/WebAuthnDeviceStorageNode`

Resource version: `1.0`

create

Usage:

```
am> create WebAuthnDeviceStorageNode --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "generateRecoveryCodes" : {
      "title" : "Generate recovery codes",
      "description" : "If enabled, the success outcome's transient state will contain a set of
 recovery codes. If this success outcome is passed into a Recovery Code Display Node, these codes will
 be presented to the user. A user may use recovery codes to bypass the WebAuthn authentication node in
 the event they have lost their authenticator. A set of recovery codes is shared among all registered
 WebAuthn authenticators, with the latest-generated set being the only valid set of codes.",
      "propertyOrder" : 10,
      "type" : "boolean",
      "exampleValue" : ""
    }
  },
  "required" : [ "generateRecoveryCodes" ]
}
```

delete

Usage:

```
am> delete WebAuthnDeviceStorageNode --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action WebAuthnDeviceStorageNode --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action WebAuthnDeviceStorageNode --realm Realm --actionName getCreatableTypes
```

listOutcomes

List the available outcomes for the node type.

Usage:

```
am> action WebAuthnDeviceStorageNode --realm Realm --body body --actionName listOutcomes
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "title" : "Some configuration of the node. This does not need to be complete against the
 configuration schema."
}
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action WebAuthnDeviceStorageNode --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query WebAuthnDeviceStorageNode --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read WebAuthnDeviceStorageNode --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update WebAuthnDeviceStorageNode --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "generateRecoveryCodes" : {
      "title" : "Generate recovery codes",
      "description" : "If enabled, the success outcome's transient state will contain a set of
 recovery codes. If this success outcome is passed into a Recovery Code Display Node, these codes will
 be presented to the user. A user may use recovery codes to bypass the WebAuthn authentication node in
 the event they have lost their authenticator. A set of recovery codes is shared among all registered
 WebAuthn authenticators, with the latest-generated set being the only valid set of codes.",
      "propertyOrder" : 10,
      "type" : "boolean",
      "exampleValue" : ""
    }
  },
  "required" : [ "generateRecoveryCodes" ]
}
```

WebAuthnRegistrationNode

Realm Operations

Resource path: `/realm-config/authentication/authenticationtrees/nodes/WebAuthnRegistrationNode`

Resource version: `1.0`

create

Usage:

```
am> create WebAuthnRegistrationNode --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "postponeDeviceProfileStorage" : {
      "title" : "Store device data in transient state",
      "description" : "If enabled, the device will not be stored directly to the user profile upon
 successful completion of the node. Rather, the device information will be placed into the transient
 state for later storage by subsequent nodes using the key 'webauthnDeviceData'. The provided
 'WebAuthn Device Storage Node' can be used for this purpose.",
      "propertyOrder" : 110,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "asScript" : {
      "title" : "Return challenge as JavaScript",
      "description" : "If enabled, the node will return its challenge as a fully encapsulated client-
side JavaScript that will interact directly with the WebAuthn API and submit the response back. If
 disabled, the node will return the challenge and associated data in a metadata node, and the custom
 UI will use that to interact with the WebAuthn API itself.",
      "propertyOrder" : 140,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "enforceRevocationCheck" : {
      "title" : "Enforce revocation check",
      "description" : "Whether to enforce the checking of revocation entries from certificates. If
 this is set to true, then any attestation certificate's trust chain MUST have a CRL or OCSP entry
 that can be verified by AM during processing. If this is is set to false, then presented certificates
 will not be checked for revocation. Certificates downloaded from the FIDO Metadata Service may not
 have a CRL/OCSP entry.",
      "propertyOrder" : 68,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "requiresResidentKey" : {
      "title" : "Username to device",
```

```
      "description" : "Requests that the username is stored by the device. Devices which do not
 support storing and providing the username will be unable to utilise the node while it is operating
 in this mode.",
      "propertyOrder" : 120,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "displayNameSharedState" : {
      "title" : "Shared state attribute for display name",
      "description" : "This field determines the value of the user's displayName, used when the user's
 username is stored in the device. If left blank, the display name will be set to the same as the
 user's username. If set to a value the corresponding shared state value will be used instead. If
 there is no value found in the shared state for the provided key, the display name will be set to the
 same as the user's username.",
      "propertyOrder" : 130,
      "type" : "string",
      "exampleValue" : ""
    },
    "userVerificationRequirement" : {
      "title" : "User verification requirement",
      "description" : "If specified as REQUIRED, authenticators that don't verify user identity are
 filtered out and should not be selectable by the user.",
      "propertyOrder" : 30,
      "type" : "string",
      "exampleValue" : ""
    },
    "storeAttestationDataInTransientState" : {
      "title" : "Store data in transient state",
      "description" : "If enabled, the information provided by the device to the node will be
 stored in the transient state for later analysis by subsequent nodes using the key 'webauthnData'.
 Additionally the type of attestation achieved (BASIC, CA, SELF, etc.) will be stored using the key
 'webauthnAttestationType'.",
      "propertyOrder" : 100,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "origins" : {
      "title" : "Origin domains",
      "description" : "A set of fully-qualified URLs of accepted origins, e.g. http://
app.example.com:443. If empty, the accepted origin is the incoming request origin.",
      "propertyOrder" : 25,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "trustStoreAlias" : {
      "title" : "Trust Store alias",
      "description" : "The alias of the realm trust store which contains the secrets necessary for
 performing validation of a supplied attestation certificate. The alias name must only contain the
 characters a-z and the . symbol.",
      "propertyOrder" : 65,
      "type" : "string",
      "exampleValue" : ""
    },
    "generateRecoveryCodes" : {
      "title" : "Generate recovery codes",
```

```
     "description" : "If enabled, the success outcome's transient state will contain a set of
recovery codes. If this success outcome is passed into a Recovery Code Display Node, these codes will
be presented to the user. A user may use recovery codes to bypass the WebAuthn authentication node in
the event they have lost their authenticator. A set of recovery codes is shared among all registered
WebAuthn authenticators, with the latest-generated set being the only valid set of codes. This will
not occur if the option to store the device data in the transient state is also selected.",
     "propertyOrder" : 90,
     "type" : "boolean",
     "exampleValue" : ""
   },
   "timeout" : {
     "title" : "Timeout",
     "description" : "The number of seconds to wait for a valid WebAuthn authenticator to be
registered before failing.",
     "propertyOrder" : 70,
     "type" : "integer",
     "exampleValue" : ""
   },
   "excludeCredentials" : {
     "title" : "Limit registrations",
     "description" : "If enabled, each authenticator may only be registered against a user's profile
once.",
     "propertyOrder" : 80,
     "type" : "boolean",
     "exampleValue" : ""
   },
   "acceptedSigningAlgorithms" : {
     "title" : "Accepted signing algorithms",
     "description" : "",
     "propertyOrder" : 50,
     "items" : {
       "type" : "string"
     },
     "type" : "array",
     "exampleValue" : ""
   },
   "relyingPartyDomain" : {
     "title" : "Relying party identifier",
     "description" : "The domain against which to register devices, if blank AM will make a best
guess at the domain.",
     "propertyOrder" : 20,
     "type" : "string",
     "exampleValue" : ""
   },
   "attestationPreference" : {
     "title" : "Preferred mode of attestation",
     "description" : "",
     "propertyOrder" : 40,
     "type" : "string",
     "exampleValue" : ""
   },
   "relyingPartyName" : {
     "title" : "Relying party",
     "description" : "The name of the Relying Party to present, this could be the name of the
organisation, realm, etc.",
     "propertyOrder" : 10,
     "type" : "string",
     "exampleValue" : ""
   },
```

```
    "authenticatorAttachment" : {
      "title" : "Authentication attachment",
      "description" : "If specified, the authenticators will be filtered out that don't match the
 attachment type. A PLATFORM authenticator is part of the device, and CROSS_PLATFORM authenticator can
 be removed from a device and used elsewhere, e.g. via USB.",
      "propertyOrder" : 60,
      "type" : "string",
      "exampleValue" : ""
    }
  },
  "required" : [ "generateRecoveryCodes", "asScript", "acceptedSigningAlgorithms",
 "postponeDeviceProfileStorage", "userVerificationRequirement", "attestationPreference",
 "authenticatorAttachment", "requiresResidentKey", "excludeCredentials", "origins",
 "storeAttestationDataInTransientState", "timeout", "relyingPartyName", "enforceRevocationCheck" ]
}
```

delete

Usage:

```
am> delete WebAuthnRegistrationNode --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action WebAuthnRegistrationNode --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action WebAuthnRegistrationNode --realm Realm --actionName getCreatableTypes
```

listOutcomes

List the available outcomes for the node type.

Usage:

```
am> action WebAuthnRegistrationNode --realm Realm --body body --actionName listOutcomes
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "title" : "Some configuration of the node. This does not need to be complete against the
 configuration schema."
}
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action WebAuthnRegistrationNode --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query WebAuthnRegistrationNode --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read WebAuthnRegistrationNode --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update WebAuthnRegistrationNode --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "postponeDeviceProfileStorage" : {
      "title" : "Store device data in transient state",
      "description" : "If enabled, the device will not be stored directly to the user profile upon
 successful completion of the node. Rather, the device information will be placed into the transient
 state for later storage by subsequent nodes using the key 'webauthnDeviceData'. The provided
 'WebAuthn Device Storage Node' can be used for this purpose.",
      "propertyOrder" : 110,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "asScript" : {
      "title" : "Return challenge as JavaScript",
      "description" : "If enabled, the node will return its challenge as a fully encapsulated client-
side JavaScript that will interact directly with the WebAuthn API and submit the response back. If
 disabled, the node will return the challenge and associated data in a metadata node, and the custom
 UI will use that to interact with the WebAuthn API itself.",
      "propertyOrder" : 140,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "enforceRevocationCheck" : {
      "title" : "Enforce revocation check",
      "description" : "Whether to enforce the checking of revocation entries from certificates. If
 this is set to true, then any attestation certificate's trust chain MUST have a CRL or OCSP entry
 that can be verified by AM during processing. If this is is set to false, then presented certificates
 will not be checked for revocation. Certificates downloaded from the FIDO Metadata Service may not
 have a CRL/OCSP entry.",
      "propertyOrder" : 68,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "requiresResidentKey" : {
      "title" : "Username to device",
      "description" : "Requests that the username is stored by the device. Devices which do not
 support storing and providing the username will be unable to utilise the node while it is operating
 in this mode.",
      "propertyOrder" : 120,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "displayNameSharedState" : {
      "title" : "Shared state attribute for display name",
      "description" : "This field determines the value of the user's displayName, used when the user's
 username is stored in the device. If left blank, the display name will be set to the same as the
 user's username. If set to a value the corresponding shared state value will be used instead. If
```

```
 there is no value found in the shared state for the provided key, the display name will be set to the
 same as the user's username.",
      "propertyOrder" : 130,
      "type" : "string",
      "exampleValue" : ""
    },
    "userVerificationRequirement" : {
      "title" : "User verification requirement",
      "description" : "If specified as REQUIRED, authenticators that don't verify user identity are
 filtered out and should not be selectable by the user.",
      "propertyOrder" : 30,
      "type" : "string",
      "exampleValue" : ""
    },
    "storeAttestationDataInTransientState" : {
      "title" : "Store data in transient state",
      "description" : "If enabled, the information provided by the device to the node will be
 stored in the transient state for later analysis by subsequent nodes using the key 'webauthnData'.
 Additionally the type of attestation achieved (BASIC, CA, SELF, etc.) will be stored using the key
 'webauthnAttestationType'.",
      "propertyOrder" : 100,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "origins" : {
      "title" : "Origin domains",
      "description" : "A set of fully-qualified URLs of accepted origins, e.g. http://
app.example.com:443. If empty, the accepted origin is the incoming request origin.",
      "propertyOrder" : 25,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "trustStoreAlias" : {
      "title" : "Trust Store alias",
      "description" : "The alias of the realm trust store which contains the secrets necessary for
 performing validation of a supplied attestation certificate. The alias name must only contain the
 characters a-z and the . symbol.",
      "propertyOrder" : 65,
      "type" : "string",
      "exampleValue" : ""
    },
    "generateRecoveryCodes" : {
      "title" : "Generate recovery codes",
      "description" : "If enabled, the success outcome's transient state will contain a set of
 recovery codes. If this success outcome is passed into a Recovery Code Display Node, these codes will
 be presented to the user. A user may use recovery codes to bypass the WebAuthn authentication node in
 the event they have lost their authenticator. A set of recovery codes is shared among all registered
 WebAuthn authenticators, with the latest-generated set being the only valid set of codes. This will
 not occur if the option to store the device data in the transient state is also selected.",
      "propertyOrder" : 90,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "timeout" : {
      "title" : "Timeout",
```

```
     "description" : "The number of seconds to wait for a valid WebAuthn authenticator to be
registered before failing.",
     "propertyOrder" : 70,
     "type" : "integer",
     "exampleValue" : ""
   },
   "excludeCredentials" : {
     "title" : "Limit registrations",
     "description" : "If enabled, each authenticator may only be registered against a user's profile
once.",
     "propertyOrder" : 80,
     "type" : "boolean",
     "exampleValue" : ""
   },
   "acceptedSigningAlgorithms" : {
     "title" : "Accepted signing algorithms",
     "description" : "",
     "propertyOrder" : 50,
     "items" : {
       "type" : "string"
     },
     "type" : "array",
     "exampleValue" : ""
   },
   "relyingPartyDomain" : {
     "title" : "Relying party identifier",
     "description" : "The domain against which to register devices, if blank AM will make a best
guess at the domain.",
     "propertyOrder" : 20,
     "type" : "string",
     "exampleValue" : ""
   },
   "attestationPreference" : {
     "title" : "Preferred mode of attestation",
     "description" : "",
     "propertyOrder" : 40,
     "type" : "string",
     "exampleValue" : ""
   },
   "relyingPartyName" : {
     "title" : "Relying party",
     "description" : "The name of the Relying Party to present, this could be the name of the
organisation, realm, etc.",
     "propertyOrder" : 10,
     "type" : "string",
     "exampleValue" : ""
   },
   "authenticatorAttachment" : {
     "title" : "Authentication attachment",
     "description" : "If specified, the authenticators will be filtered out that don't match the
attachment type. A PLATFORM authenticator is part of the device, and CROSS_PLATFORM authenticator can
be removed from a device and used elsewhere, e.g. via USB.",
     "propertyOrder" : 60,
     "type" : "string",
     "exampleValue" : ""
   }
 },
 "required" : [ "generateRecoveryCodes", "asScript", "acceptedSigningAlgorithms",
"postponeDeviceProfileStorage", "userVerificationRequirement", "attestationPreference",
```

```
 "authenticatorAttachment", "requiresResidentKey", "excludeCredentials", "origins",
 "storeAttestationDataInTransientState", "timeout", "relyingPartyName", "enforceRevocationCheck" ]
}
```

WebAuthnUserDevices

Realm Operations

The WebAuthn devices service is responsible for exposing functions to change the collection of WebAuthn authentication devices. The supported methods are update, delete, query

Resource path: `/users/{user}/devices/2fa/webauthn`

Resource version: `1.0`

delete

Delete WebAuthn user device

Usage:

```
am> delete WebAuthnUserDevices --realm Realm --id id --user user
```

Parameters:

`--id`

The unique identifier for the resource.

`--user`

The WebAuthn devices service is responsible for exposing functions to change the collection of WebAuthn authentication devices. The supported methods are update, delete, query

query

Query the user's WebAuthn devices

Usage:

```
am> query WebAuthnUserDevices --realm Realm --filter filter --user user
```

Parameters:

`--filter`

A CREST formatted query filter, where "true" will query all. Fields that can be queried: [*]

--user

The WebAuthn devices service is responsible for exposing functions to change the collection of WebAuthn authentication devices. The supported methods are update, delete, query

update

Update an existing WebAuthn user device

Usage:

```
am> update WebAuthnUserDevices --realm Realm --id id --body body --user user
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "$schema" : "http://json-schema.org/draft-04/schema#",
  "description" : "User devices schema that is used for WebAuthn authentication devices",
  "type" : "object",
  "title" : "User devices schema",
  "properties" : {
    "deviceName" : {
      "type" : "string",
      "title" : "Device Name",
      "description" : "The name of the WebAuthn device."
    },
    "uuid" : {
      "type" : "string",
      "title" : "UUID",
      "description" : "The unique identifier for this device."
    }
  }
}
```

--user

The WebAuthn devices service is responsible for exposing functions to change the collection of WebAuthn authentication devices. The supported methods are update, delete, query

WebhookService

Realm Operations

Resource path: `/realm-config/webhooks`

Resource version: `1.0`

create

Usage:

```
am> create WebhookService --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "body" : {
      "title" : "Body",
      "description" : "The webhook body to be sent in the http request.",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "headers" : {
      "title" : "Headers",
      "description" : "The webhook headers added to the http request.",
      "propertyOrder" : 300,
      "required" : true,
      "patternProperties" : {
        ".*" : {
          "type" : "string"
        }
      },
      "type" : "object",
      "exampleValue" : ""
    },
    "url" : {
      "title" : "Url",
      "description" : "The webhook url that is used to create the http call for this webhook.",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }
```

```
}
```

delete

Usage:

```
am> delete WebhookService --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action WebhookService --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action WebhookService --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action WebhookService --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query WebhookService --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read WebhookService --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update WebhookService --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "body" : {
      "title" : "Body",
      "description" : "The webhook body to be sent in the http request.",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "headers" : {
      "title" : "Headers",
      "description" : "The webhook headers added to the http request.",
      "propertyOrder" : 300,
```

```
      "required" : true,
      "patternProperties" : {
        ".*" : {
          "type" : "string"
        }
      },
      "type" : "object",
      "exampleValue" : ""
    },
    "url" : {
      "title" : "Url",
      "description" : "The webhook url that is used to create the http call for this webhook.",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
```

Global Operations

Resource path: `/global-config/webhooks`

Resource version: `1.0`

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action WebhookService --global --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action WebhookService --global --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action WebhookService --global --actionName nextdescendents
```

read

Usage:

```
am> read WebhookService --global
```

update

Usage:

```
am> update WebhookService --global --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object"
}
```

WindowsDesktopSsoModule

Realm Operations

Resource path: `/realm-config/authentication/modules/windowsdesktopsso`

Resource version: `1.0`

create

Usage:

```
am> create WindowsDesktopSsoModule --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "trustedKerberosRealms" : {
      "title" : "Trusted Kerberos realms",
      "description" : "List of trusted Kerberos realms for User Kerberos tickets.<br><br>If realms are
 configured, then Kerberos tickets are only accepted if the realm part of the UserPrincipalName of the
 Users Kerberos ticket matches a realm from the list.",
      "propertyOrder" : 700,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "authenticationLevel" : {
      "title" : "Authentication Level",
      "description" : "The authentication level associated with this module.<br><br>Each
 authentication module has an authentication level that can be used to indicate the level of security
 associated with the module; 0 is the lowest (and the default).",
      "propertyOrder" : 600,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "kerberosServerName" : {
      "title" : "Kerberos Server Name",
      "description" : "The hostname/IP address of the Kerberos (Active Directory) server.",
      "propertyOrder" : 400,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "principalName" : {
      "title" : "Service Principal",
      "description" : "The name of the Kerberos principal used during authentication<br><br>This
 principal must match the name used in the keytab file created from the Active Directory server.<br/
>The format of the field is as follows:<br/><br/><code>HTTP/openam.forgerock.com@AD_DOMAIN.COM</
code>",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "kerberosServiceIsinitiator" : {
      "title" : "isInitiator",
      "description" : "Configuration used for JDK Kerbrose LoginModule. True, if initiator. False, if
 acceptor only. Default is true",
      "propertyOrder" : 900,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "keytabFileName" : {
```

```
      "title" : "Keytab File Name",
      "description" : "The path of the AD keytab file<br><br>This is the absolute pathname of the AD
 keytab file. The keytab file is generated by the Active Directory server.",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "kerberosRealm" : {
      "title" : "Kerberos Realm",
      "description" : "The name of the Kerberos (Active Directory) realm used for authentication",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "returnPrincipalWithDomainName" : {
      "title" : "Return Principal with Domain Name",
      "description" : "Returns the fully qualified name of the authenticated user rather than just the
 username.",
      "propertyOrder" : 500,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "lookupUserInRealm" : {
      "title" : "Search for the user in the realm",
      "description" : "Validate that the user has a matched user profile configured in the data
 store.<br><br>If this option is enabled, the module validates whether the account corresponds to a
 user profile in the Data Store for the realm. The attributes to perform the search are configured
 under <i>Access Control > Realm Name > Authentication > All Core settings > Alias Search Attribute
 Name</i>.",
      "propertyOrder" : 800,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    }
  }
}
```

delete

Usage:

```
am> delete WindowsDesktopSsoModule --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action WindowsDesktopSsoModule --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action WindowsDesktopSsoModule --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action WindowsDesktopSsoModule --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query WindowsDesktopSsoModule --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read WindowsDesktopSsoModule --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update WindowsDesktopSsoModule --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "trustedKerberosRealms" : {
      "title" : "Trusted Kerberos realms",
      "description" : "List of trusted Kerberos realms for User Kerberos tickets.<br><br>If realms are
 configured, then Kerberos tickets are only accepted if the realm part of the UserPrincipalName of the
 Users Kerberos ticket matches a realm from the list.",
      "propertyOrder" : 700,
      "required" : true,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "authenticationLevel" : {
      "title" : "Authentication Level",
      "description" : "The authentication level associated with this module.<br><br>Each
 authentication module has an authentication level that can be used to indicate the level of security
 associated with the module; 0 is the lowest (and the default).",
      "propertyOrder" : 600,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "kerberosServerName" : {
      "title" : "Kerberos Server Name",
      "description" : "The hostname/IP address of the Kerberos (Active Directory) server.",
      "propertyOrder" : 400,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "principalName" : {
      "title" : "Service Principal",
      "description" : "The name of the Kerberos principal used during authentication<br><br>This
 principal must match the name used in the keytab file created from the Active Directory server.<br/
>The format of the field is as follows:<br/><br/><code>HTTP/openam.forgerock.com@AD_DOMAIN.COM</
code>",
      "propertyOrder" : 100,
      "required" : true,
```

```
      "type" : "string",
      "exampleValue" : ""
    },
    "kerberosServiceIsinitiator" : {
      "title" : "isInitiator",
      "description" : "Configuration used for JDK Kerbrose LoginModule. True, if initiator. False, if
 acceptor only. Default is true",
      "propertyOrder" : 900,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "keytabFileName" : {
      "title" : "Keytab File Name",
      "description" : "The path of the AD keytab file<br><br>This is the absolute pathname of the AD
 keytab file. The keytab file is generated by the Active Directory server.",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "kerberosRealm" : {
      "title" : "Kerberos Realm",
      "description" : "The name of the Kerberos (Active Directory) realm used for authentication",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "returnPrincipalWithDomainName" : {
      "title" : "Return Principal with Domain Name",
      "description" : "Returns the fully qualified name of the authenticated user rather than just the
 username.",
      "propertyOrder" : 500,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "lookupUserInRealm" : {
      "title" : "Search for the user in the realm",
      "description" : "Validate that the user has a matched user profile configured in the data
 store.<br><br>If this option is enabled, the module validates whether the account corresponds to a
 user profile in the Data Store for the realm. The attributes to perform the search are configured
 under <i>Access Control > Realm Name > Authentication > All Core settings > Alias Search Attribute
 Name</i>.",
      "propertyOrder" : 800,
      "required" : true,
      "type" : "boolean",
      "exampleValue" : ""
    }
  }
}
```


Global Operations

Resource path: `/global-config/authentication/modules/windowsdesktopsso`

Resource version: `1.0`

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action WindowsDesktopSsoModule --global --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action WindowsDesktopSsoModule --global --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action WindowsDesktopSsoModule --global --actionName nextdescendents
```

read

Usage:

```
am> read WindowsDesktopSsoModule --global
```

update

Usage:

```
am> update WindowsDesktopSsoModule --global --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "defaults" : {
      "properties" : {
        "kerberosRealm" : {
```

```
          "title" : "Kerberos Realm",
          "description" : "The name of the Kerberos (Active Directory) realm used for authentication",
          "propertyOrder" : 300,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "kerberosServiceIsinitiator" : {
          "title" : "isInitiator",
          "description" : "Configuration used for JDK Kerbrose LoginModule. True, if initiator. False,
if acceptor only. Default is true",
          "propertyOrder" : 900,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "trustedKerberosRealms" : {
          "title" : "Trusted Kerberos realms",
          "description" : "List of trusted Kerberos realms for User Kerberos tickets.<br><br>If realms
are configured, then Kerberos tickets are only accepted if the realm part of the UserPrincipalName of
the Users Kerberos ticket matches a realm from the list.",
          "propertyOrder" : 700,
          "required" : true,
          "items" : {
            "type" : "string"
          },
          "type" : "array",
          "exampleValue" : ""
        },
        "kerberosServerName" : {
          "title" : "Kerberos Server Name",
          "description" : "The hostname/IP address of the Kerberos (Active Directory) server.",
          "propertyOrder" : 400,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "keytabFileName" : {
          "title" : "Keytab File Name",
          "description" : "The path of the AD keytab file<br><br>This is the absolute pathname of the
AD keytab file. The keytab file is generated by the Active Directory server.",
          "propertyOrder" : 200,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "authenticationLevel" : {
          "title" : "Authentication Level",
          "description" : "The authentication level associated with this module.<br><br>Each
authentication module has an authentication level that can be used to indicate the level of security
associated with the module; 0 is the lowest (and the default).",
          "propertyOrder" : 600,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "lookupUserInRealm" : {
          "title" : "Search for the user in the realm",
```

```
          "description" : "Validate that the user has a matched user profile configured in the data
 store.<br><br>If this option is enabled, the module validates whether the account corresponds to a
 user profile in the Data Store for the realm. The attributes to perform the search are configured
 under <i>Access Control > Realm Name > Authentication > All Core settings > Alias Search Attribute
 Name</i>.",
          "propertyOrder" : 800,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        },
        "principalName" : {
          "title" : "Service Principal",
          "description" : "The name of the Kerberos principal used during authentication<br><br>This
 principal must match the name used in the keytab file created from the Active Directory server.<br/
>The format of the field is as follows:<br/><br/><code>HTTP/openam.forgerock.com@AD_DOMAIN.COM</
code>",
          "propertyOrder" : 100,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "returnPrincipalWithDomainName" : {
          "title" : "Return Principal with Domain Name",
          "description" : "Returns the fully qualified name of the authenticated user rather than just
 the username.",
          "propertyOrder" : 500,
          "required" : true,
          "type" : "boolean",
          "exampleValue" : ""
        }
      },
      "type" : "object",
      "title" : "Realm Defaults"
    }
  }
}
```


WindowsNtModule

Realm Operations

Resource path: `/realm-config/authentication/modules/windowsnt`

Resource version: `1.0`

create

Usage:

```
am> create WindowsNtModule --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "sambaConfigurationFileName" : {
      "title" : "Samba Configuration File Name",
      "description" : "The path to the Samba configuration file.<br><br>The Windows NT authentication
 module uses the <code>smbclient</code> command to validate the user credentials against the Windows
 domain controller. <br/><br/>For example: <code>/opt/openam/smb.conf</code><br/><br/><i>NB </i>The
 <code>smbclient</code> command must be available in the <code>PATH</code> environmental variable
 associated with OpenAM.",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "authenticationDomain" : {
      "title" : "Authentication Domain",
      "description" : "The name of the Windows Domain used for authentication",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "authenticationLevel" : {
      "title" : "Authentication Level",
      "description" : "The authentication level associated with this module.<br><br>Each
 authentication module has an authentication level that can be used to indicate the level of security
 associated with the module; 0 is the lowest (and the default). ",
      "propertyOrder" : 400,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "authenticationHost" : {
      "title" : "Authentication Host",
      "description" : "The name of the Windows NT Domain Controller.",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
```

delete

Usage:

```
am> delete WindowsNtModule --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action WindowsNtModule --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action WindowsNtModule --realm Realm --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action WindowsNtModule --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query WindowsNtModule --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read WindowsNtModule --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update WindowsNtModule --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "sambaConfigurationFileName" : {
      "title" : "Samba Configuration File Name",
      "description" : "The path to the Samba configuration file.<br><br>The Windows NT authentication
 module uses the <code>smbclient</code> command to validate the user credentials against the Windows
 domain controller. <br/><br/>For example: <code>/opt/openam/smb.conf</code><br/><br/><i>NB </i>The
 <code>smbclient</code> command must be available in the <code>PATH</code> environmental variable
 associated with OpenAM.",
      "propertyOrder" : 300,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "authenticationDomain" : {
      "title" : "Authentication Domain",
      "description" : "The name of the Windows Domain used for authentication",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "authenticationLevel" : {
```

```
      "title" : "Authentication Level",
      "description" : "The authentication level associated with this module.<br><br>Each
 authentication module has an authentication level that can be used to indicate the level of security
 associated with the module; 0 is the lowest (and the default). ",
      "propertyOrder" : 400,
      "required" : true,
      "type" : "integer",
      "exampleValue" : ""
    },
    "authenticationHost" : {
      "title" : "Authentication Host",
      "description" : "The name of the Windows NT Domain Controller.",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
```

Global Operations

Resource path: `/global-config/authentication/modules/windowsnt`

Resource version: `1.0`

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action WindowsNtModule --global --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action WindowsNtModule --global --actionName getCreatableTypes
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action WindowsNtModule --global --actionName nextdescendents
```

read

Usage:

```
am> read WindowsNtModule --global
```

update

Usage:

```
am> update WindowsNtModule --global --body body
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "defaults" : {
      "properties" : {
        "authenticationHost" : {
          "title" : "Authentication Host",
          "description" : "The name of the Windows NT Domain Controller.",
          "propertyOrder" : 200,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "authenticationDomain" : {
          "title" : "Authentication Domain",
          "description" : "The name of the Windows Domain used for authentication",
          "propertyOrder" : 100,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        },
        "authenticationLevel" : {
          "title" : "Authentication Level",
          "description" : "The authentication level associated with this module.<br><br>Each
 authentication module has an authentication level that can be used to indicate the level of security
 associated with the module; 0 is the lowest (and the default). ",
          "propertyOrder" : 400,
          "required" : true,
          "type" : "integer",
          "exampleValue" : ""
        },
        "sambaConfigurationFileName" : {
          "title" : "Samba Configuration File Name",
          "description" : "The path to the Samba configuration file.<br><br>The Windows NT
 authentication module uses the <code>smbclient</code> command to validate the user credentials
 against the Windows domain controller. <br/><br/>For example: <code>/opt/openam/smb.conf</code><br/
```

```
><br/><i>NB </i>The <code>smbclient</code> command must be available in the <code>PATH</code>
 environmental variable associated with OpenAM.",
          "propertyOrder" : 300,
          "required" : true,
          "type" : "string",
          "exampleValue" : ""
        }
      },
      "type" : "object",
      "title" : "Realm Defaults"
    }
  }
}
```

WriteFederationInformation

Realm Operations

Resource path: `/realm-config/authentication/authenticationtrees/nodes/product-WriteFederationInformationNode`

Resource version: `1.0`

create

Usage:

```
am> create WriteFederationInformation --realm Realm --id id --body body
```

Parameters:

`--id`

The unique identifier for the resource.

`--body`

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "required" : [ ]
}
```

delete

Usage:

```
am> delete WriteFederationInformation --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action WriteFederationInformation --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action WriteFederationInformation --realm Realm --actionName getCreatableTypes
```

listOutcomes

List the available outcomes for the node type.

Usage:

```
am> action WriteFederationInformation --realm Realm --body body --actionName listOutcomes
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "title" : "Some configuration of the node. This does not need to be complete against the
 configuration schema."
}
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action WriteFederationInformation --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query WriteFederationInformation --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read WriteFederationInformation --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update WriteFederationInformation --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "required" : [ ]
}
```

WsEntity

Realm Operations

Resource path: `/realm-config/federation/entityproviders/ws`

Resource version: `1.0`

create

Usage:

```
am> create WsEntity --realm Realm --id id --body body
```

Parameters:

`--id`

The unique identifier for the resource.

`--body`

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "entityConfig" : {
      "title" : "Entity Configuration",
      "description" : "",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "metadata" : {
      "title" : "Metadata",
      "description" : "",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
```

delete

Usage:

```
am> delete WsEntity --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query WsEntity --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read WsEntity --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update WsEntity --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "entityConfig" : {
      "title" : "Entity Configuration",
      "description" : "",
      "propertyOrder" : 200,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    },
    "metadata" : {
      "title" : "Metadata",
      "description" : "",
      "propertyOrder" : 100,
      "required" : true,
      "type" : "string",
      "exampleValue" : ""
    }
  }
}
```

ZeroPageLoginCollector

Realm Operations

Resource path: `/realm-config/authentication/authenticationtrees/nodes/ZeroPageLoginNode`

Resource version: `1.0`

create

Usage:

```
am> create ZeroPageLoginCollector --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "referrerWhiteList" : {
      "title" : "Referer Whitelist",
      "description" : "",
      "propertyOrder" : 400,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "allowWithoutReferer" : {
      "title" : "Allow Without Referer",
      "description" : "",
      "propertyOrder" : 300,
      "type" : "boolean",
      "exampleValue" : ""
    },
    "passwordHeader" : {
      "title" : "Password Header Name",
      "description" : "",
      "propertyOrder" : 200,
      "type" : "string",
      "exampleValue" : ""
    },
    "usernameHeader" : {
      "title" : "Username Header Name",
      "description" : "",
      "propertyOrder" : 100,
      "type" : "string",
      "exampleValue" : ""
    }
  },
  "required" : [ "referrerWhiteList", "passwordHeader", "usernameHeader", "allowWithoutReferer" ]
}
```

delete

Usage:

```
am> delete ZeroPageLoginCollector --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

getAllTypes

Obtain the collection of all secondary configuration types related to the resource.

Usage:

```
am> action ZeroPageLoginCollector --realm Realm --actionName getAllTypes
```

getCreatableTypes

Obtain the collection of secondary configuration types that have yet to be added to the resource.

Usage:

```
am> action ZeroPageLoginCollector --realm Realm --actionName getCreatableTypes
```

listOutcomes

List the available outcomes for the node type.

Usage:

```
am> action ZeroPageLoginCollector --realm Realm --body body --actionName listOutcomes
```

Parameters:

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "title" : "Some configuration of the node. This does not need to be complete against the
 configuration schema."
}
```

nextdescendents

Obtain the collection of secondary configuration instances that have been added to the resource.

Usage:

```
am> action ZeroPageLoginCollector --realm Realm --actionName nextdescendents
```

query

Get the full list of instances of this collection. This query only supports `_queryFilter=true` filter.

Usage:

```
am> query ZeroPageLoginCollector --realm Realm --filter filter
```

Parameters:

--filter

A CREST formatted query filter, where "true" will query all.

read

Usage:

```
am> read ZeroPageLoginCollector --realm Realm --id id
```

Parameters:

--id

The unique identifier for the resource.

update

Usage:

```
am> update ZeroPageLoginCollector --realm Realm --id id --body body
```

Parameters:

--id

The unique identifier for the resource.

--body

The resource in JSON format, described by the following JSON schema:

```
{
  "type" : "object",
  "properties" : {
    "referrerWhiteList" : {
      "title" : "Referer Whitelist",
      "description" : "",
      "propertyOrder" : 400,
      "items" : {
        "type" : "string"
      },
      "type" : "array",
      "exampleValue" : ""
    },
    "allowWithoutReferer" : {
      "title" : "Allow Without Referer",
      "description" : "",
      "propertyOrder" : 300,
      "type" : "boolean",
      "exampleValue" : ""
```

```
    },
    "passwordHeader" : {
      "title" : "Password Header Name",
      "description" : "",
      "propertyOrder" : 200,
      "type" : "string",
      "exampleValue" : ""
    },
    "usernameHeader" : {
      "title" : "Username Header Name",
      "description" : "",
      "propertyOrder" : 100,
      "type" : "string",
      "exampleValue" : ""
    }
  },
  "required" : [ "referrerWhiteList", "passwordHeader", "usernameHeader", "allowWithoutReferer" ]
}
```