Reference

/ ForgeRock Access Management 7.1.4

Latest update: 7.1.4

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

Abstract

Reference documentation for ForgeRock® Access Management (AM). ForgeRock Access Management provides intelligent authentication, authorization, federation, and single sign-on functionality.

Table of Contents

Overview

This reference is written for access management designers, developers, and administrators using ForgeRock Access Management tools, logs, and global configuration.

Quick Start

 Command-line Tools Learn about the various AM command-line tools, such as **ampassword** and **ssoadm**.	 Global Configuration Reference Browse through the properties available when configuring an AM instance at the global level.	 Standards Support View the wide range of RFCs, standards, specifications, and internet-drafts supported by AM.
 Ports Used Ensure your environment allows traffic to the ports that AM requires for operation.	 Endpoints Discover the endpoints that AM provides, and decide if they are required in your deployment.	 Log Files and Messages View information about the different log files and messages AM outputs when using the classic Logging Service.

ForgeRock Access Management provides two online API references for developers:

- **Access Management Public API Javadocs**. For a reference to the Access Management Java API, see the Javadoc.
- **ForgeRock® Common Rest API**. Access Management provides an online reference to the Common REST API. Access the API on the AM console by pointing to the following URL:

```
https://openam.example.com:8443/openam/ui-admin/#api/explorer
```

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

Command Line Tools

This chapter provides a reference for the ForgeRock Access Management command line tools.

ampassword

Change passwords for the AM Administrator.

`ampassword` {options}

Description

This command allows you to change passwords held in the configuration store, and to encrypt passwords.

Options

The following options are supported.

`-a | --admin [ -o | --old` ***`old-password-file`*** **`-n | --new`** ***`new-password-file`*** **`]`**

Change the password for `amAdmin` from the value stored in *old-password-file* to the value stored in *new-password-file*.

`-p | --proxy [ -o | --old` ***`old-password-file`*** **`-n | --new`** ***`new-password-file`*** **`]`**

Change the password for the proxy administrator from the value stored in *old-password-file* to the value stored in *new-password-file*.

The proxy administrator password is shown encrypted in the output from **ssoadm get-svrcfg-xml**.

`-e | --encrypt [` ***`password-file`*** **`]`**

Display the password value provided encrypted with the key generated during AM installation.

`-h | --help`

Display the usage message.

Examples

The following example encrypts the password contained within a text file.

- Create a text file, for example `$HOME/.pwd.txt`, containing the password string on a single line.
- Encrypt the password by using the **ampassword** command:

```
$ ampassword -e $HOME/.pwd.txt
AQICkZs3qy5QUCXir9tebIEEZYGFXI2lCC4B
```

amverifyarchive

Check AM log archives for tampering.

`amverifyarchive` {options}

Description

This command checks log archive integrity.

Options

The following options are required.

`-l` *`logName`*

Verify log files of the specified type. To specify an individual log rather than a type, provide the entire log file name.

`-p` *`path`*

Path to log files to verify.

`-u` *`userName`*

User who can read log files.

`-w` *`password`*

Password of the user who can read log files.

Examples

The following example checks the `amConsole` logs.

```
$ amverifyarchive \
 -l amConsole \
 -p /path/to/openam/var/audit/ \
 -u amadmin \
 -w password
```

configurator.jar

Install or upgrade AM using a configuration file.

`configurator.jar` {options}

Description

This executable .jar file, openam-configurator-tool-14.1.3.19.jar, lets you perform silent installation, configuring a deployed AM server by applying settings from a configuration file.

Options

The following options are supported.

`-f | --file *configuration-file*`

Configure a deployed AM web application archive using the specified configuration file. Installation and upgrade configuration files are described in the sections below.

`--acceptLicense`

Auto-accept the software license agreement and suppress the display of the licence acceptance screen to the user. If the configuration file contains the `ACCEPT_LICENSES` property, it will have precedence over the command-line option.

`-? | --help`

Display the usage message.

Installation Configuration File

Base your configuration on the `sampleconfiguration` file delivered with AM, and using the hints in this section, or the comments included in the file.

Server Properties

These properties pertain to the AM server instance.

SERVER_URL

URL to the web container where you want AM to run, such as `http://openam.example.com:8080`

DEPLOYMENT_URI

URI where you want to deploy AM on the web container, such as `/openam`

BASE_DIR

Configuration directory where AM stores files and embedded configuration directory server, such as `$HOME/openam`

locale

The user locale, such as `en_GB`

PLATFORM_LOCALE

The locale of the AM server, such as `en_US`

AM_ENC_KEY

The password encryption key, which must be the same on all servers in a multi-server installation, such as `06QWwHPO4os+zEz3Nqn/2daAYWyiFE32`. If left blank, installing AM generates a random password encryption key that you can view in the AM console, under Deployment > Servers > *Server Name* > Security.

ADMIN_PWD

Password of the AM administrator user `amAdmin`, which must be at least 8 characters in length and must match that of other servers in a multiserver deployment

COOKIE_DOMAIN

Name of the trusted DNS domain AM returns to a browser when it grants a session ID to a user. By default, it is set to the full URL that was used to access the configurator, such as `example.com`.

ACCEPT_LICENSES

Optional boolean property that can be set to always auto-accept the software license agreement and suppress the display of the license acceptance screen to the user. A value of `true` auto-accepts the license; any other value will be assumed to equal `false`, resulting in the presentation of the license. Default value is `false`. This property takes precedence over the `--acceptLicense` option, which can also be passed in to the application with the openam-configurator-tool-14.1.3.19.jar file.

Configuration Store Properties

These properties pertain to the directory server where AM stores its configuration.

DATA_STORE

Type of the configuration data store. The value `embedded` means set up AM with an embedded, DS configuration store. The value `dirServer` means an external directory server, such as ForgeRock Directory Services, or Oracle Directory Server Enterprise Edition. If you set this to `dirServer`, and the configuration store contains the configuration of other AM servers, then the server is added to the existing multiserver installation.

DIRECTORY_SSL

To use LDAP without SSL, set this to `SIMPLE`. To use LDAP with SSL, set this to `SSL`.

DIRECTORY_SERVER

Fully qualified domain name of the configuration store directory server host, such as `opendj.example.com`

DIRECTORY_PORT

LDAP or LDAPS port number for the configuration store directory server, such as 389 or 636

DIRECTORY_ADMIN_PORT

Administration port number for the configuration store directory server, such as 4444

DIRECTORY_JMX_PORT

Java Management eXtension port number, such as `1689`, used with the DS embedded configuration store

ROOT_SUFFIX

Root suffix distinguished name (DN) for the configuration store, such as `o=openam`

DS_DIRMGRDN

Distinguished name of the directory manager of the configuration store, such as `uid=admin`

DS_DIRMGRPASSWD

Password for the directory manager of the configuration store

User Data Store Properties

These properties pertain to the directory server where AM stores user profiles. If you do not include these properties, or you leave these properties commented out, then AM uses the same directory server as it uses for the configuration store.

USERSTORE_TYPE

The type of directory server used. Valid values include the following.

- `LDAPv3ForOpenDS`: ForgeRock 0penDJ or Sun OpenDS
- `LDAPv3ForAD`: Active Directory with host and port settings
- `LDAPv3ForADDC`: Active Directory with a Domain Name setting
- `LDAPv3ForADAM`: Active Directory Lightweight Directory Services[1]
- `LDAPv3ForODSEE`: Sun Java System Directory Server
- `LDAPv3ForTivoli`: IBM Tivoli Directory Server

USERSTORE_SSL

To use LDAP without SSL, set this to `SIMPLE`. To use LDAP with SSL, set this to `SSL`.

USERSTORE_DOMAINNAME

If `USERSTORE_TYPE` is `LDAPv3ForADDC`, you set this to the Active Directory Domain Name, such as `ad.example.com`, and then set only the `USERSTORE_SSL`, `USERSTORE_MGRDN`, and `USERSTORE_PASSWD` additional parameters. This lets Active Directory use DNS to retrieve service locations. Otherwise, do not use.

USERSTORE_HOST

Fully qualified domain name of the user data store directory server, such as `opendj.example.com`

USERSTORE_PORT

Port number of the user data store. Default for LDAP is 389, and for LDAP over SSL is 636.

USERSTORE_SUFFIX

Root suffix distinguished name for the user data in the directory, such as `dc=example,dc=com`

USERSTORE_MGRDN

Distinguished name of the directory manager of the user data store, such as `uid=admin`

USERSTORE_PASSWD

Password for the directory manager of the user data store

Site Properties

These properties pertain when you configure multiple AM servers in a site deployment, where a load balancer spreads request across multiple servers.

[1] Formerly known as *Active Directory Application Mode* (ADAM).

LB_SITE_NAME

The name of the AM site

LB_PRIMARY_URL

The load balancer URL for the site, such as `http://lb.example.com:80/openam`.

Upgrade Configuration File

Base your configuration on the `sampleconfiguration` file delivered with AM, and using the hints in this section, or the comments included in the file.

Upgrade Properties

SERVER_URL

URL to the web container where AM runs, such as `http://openam.example.com:8080`

DEPLOYMENT_URI

URI where AM is deployed on the web container, such as `/openam`

ACCEPT_LICENSES

Optional boolean property that can be set to always auto-accept the software license agreement and suppress displaying the license acceptance screen to the user. A value of `true` auto-accepts the license; any other value will be assumed to equal `false`, resulting in the presentation of the license. Default value is `false`. This property takes precedence over the `--acceptLicense` option, which can also be passed in to the application with the openam-configurator-tool-14.1.3.19.jar file.

Examples

The following example shows a configuration file to install a server with an external configuration and identity data stores:

```
# Server properties, AM_ENC_KEY="" means generate random key
SERVER_URL=https://openam.example.com:8443
DEPLOYMENT_URI=/openam
BASE_DIR=$HOME/openam
locale=en_US
PLATFORM_LOCALE=en_US
AM_ENC_KEY=
ADMIN_PWD=change3me
COOKIE_DOMAIN=openam.example.com
ACCEPT_LICENSES=true

# External configuration data store
DATA_STORE=dirServer
```

```
DIRECTORY_SSL=SSL
DIRECTORY_SERVER=opendj.example.com
DIRECTORY_PORT=1636
DIRECTORY_ADMIN_PORT=4444
DIRECTORY_JMX_PORT=1689
ROOT_SUFFIX=o=openam
DS_DIRMGRDN=uid=admin
DS_DIRMGRPASSWD=chang3me

# External DS-based user data store
USERSTORE_TYPE=LDAPv3ForOpenDS
USERSTORE_SSL=SSL
#USERSTORE_DOMAINNAME=ad.example.com
USERSTORE_HOST=opendj.example.com
USERSTORE_PORT=1636
USERSTORE_SUFFIX=dc=example,dc=com
USERSTORE_MGRDN=uid=admin
USERSTORE_PASSWD=secret12

# Uncomment to specify the site for the first server in a site configuration
#LB_SITE_NAME=lb
#LB_PRIMARY_URL=http://lb.example.com:80/openam
```

The following example shows a configuration file to install the second server in a site configuration.

```
# Server properties, AM_ENC_KEY from first server
SERVER_URL=https://server2.example.com:8443
DEPLOYMENT_URI=/openam
BASE_DIR=$HOME/openam
locale=en_US
PLATFORM_LOCALE=en_US
AM_ENC_KEY=O6QWwHPO4os+zEz3Nqn/2daAYWyiFE32
ADMIN_PWD=change3me
AMLDAPUSERPASSWD=secret12
COOKIE_DOMAIN=openam.example.com
ACCEPT_LICENSES=true

# External configuration data store
DATA_STORE=dirServer
DIRECTORY_SSL=SSL
DIRECTORY_SERVER=opendj.example.com
DIRECTORY_PORT=1636
DIRECTORY_ADMIN_PORT=4444
DIRECTORY_JMX_PORT=1689
ROOT_SUFFIX=o=openam
DS_DIRMGRDN=uid=admin
DS_DIRMGRPASSWD=chang3me

# External DS-based user data store
USERSTORE_TYPE=LDAPv3ForOpenDS
USERSTORE_SSL=SSL
#USERSTORE_DOMAINNAME=ad.example.com
USERSTORE_HOST=opendj.example.com
USERSTORE_PORT=1636
USERSTORE_SUFFIX=dc=example,dc=com
USERSTORE_MGRDN=uid=admin
USERSTORE_PASSWD=secret12
```

```
# Site properties
LB_SITE_NAME=lb
LB_PRIMARY_URL=http://lb.example.com:80/openam
```

The following example shows a configuration file to upgrade an AM server:

```
SERVER_URL=https://openam.example.com:8443
DEPLOYMENT_URI=/openam
ACCEPT_LICENSES=true
```

The following example uses a configuration file with the `--acceptLicense` option on the command line.

```
$ java \
 -jar openam-configurator-tool-14.1.3.19.jar \
 -f config.file \
 --acceptLicense
```

upgrade.jar

upgrade AM using a configuration file

`upgrade.jar` {options}

Description

This executable jar file, openam-upgrade-tool-14.1.3.19.jar, lets you perform a silent upgrade on a deployed AM server by applying settings from a configuration file or using arguments. This capability allows you to include the `upgrade.jar` from a command line or in an upgrade script.

Options

The following options are supported.

`-f | --file configuration-file`

Upgrade a deployed AM web application archive using the specified configuration file. Upgrade configuration files are described in the sections below. Also, you can specify the system properties on the command line, instead of using the configuration file. See Example 2 below.

`--acceptLicense`

Auto-accept the software license agreement and suppress the display of the licence acceptance screen to the user. If the configuration file contains the `ACCEPT_LICENSES` property, it will have precedence over the command-line option.

`-? | --help`

Display the usage message.

Upgrade Configuration File

Base your configuration on the `sampleupgrade` file delivered with AM, and using the hints in this section, or the comments included in the file.

Upgrade Properties

SERVER_URL

URL to the web container where AM runs, such as `http://openam.example.com:8080`.

DEPLOYMENT_URI

URI where AM is deployed on the web container, such as `/openam`.

ACCEPT_LICENSES

Optional boolean property that can be set to always auto-accept the software license agreement and suppress displaying the license acceptance screen to the user. A value of `true` auto-accepts the license; any other value will be assumed to equal `false`, resulting in the presentation of the license. Default value is `false`. This property takes precedence over the `--acceptLicense` option, which can also be passed in to the application with the openam-upgrade-tool-14.1.3.19.jar file.

Examples

The following example shows a configuration file and the commands to upgrade a server using the `upgrade.jar`. The configuration file is saved as `/tmp/upgrade.txt`.

```
SERVER_URL=http://openam.example.com:8080
DEPLOYMENT_URI=/openam
ACCEPT_LICENSES=true
```

```
$JAVA_HOME/bin/java -jar ~/openam/tools/openam-upgrade-tool-14.1.3.19.jar \
 -f /tmp/upgrade.txt
```

The following example shows how to specify system properties with the `upgrade.jar`.

```
SERVER_URL=http://openam.example.com:8080
DEPLOYMENT_URI=/openam
ACCEPT_LICENSES=true
```

```
$JAVA_HOME/bin/java -jar ~/openam/tools/openam-upgrade-tool-14.1.3.19.jar \
 -DSERVER_URL=http://openam.example.com:8080 -DDEPLOYMENT_URI=/openam
```

The following example shows the use of the `--acceptLicense` option with the `upgrade.jar`.

```
SERVER_URL=http://openam.example.com:8080
DEPLOYMENT_URI=/openam
```

```
$JAVA_HOME/bin/java -jar ~/openam/tools/openam-upgrade-tool-14.1.3.19.jar \
 -DSERVER_URL=http://openam.example.com:8080 -DDEPLOYMENT_URI=/openam \
 --acceptLicense
```

ssoadm

Configure OpenAM core services.

`ssoadm` [*subcommand*] [options]

Description

The **ssoadm** command provides a rich command-line interface for configuring OpenAM core services.

Also see the *Installation Guide* procedure, *To Set Up Administration Tools* in the *Installation Guide* for instructions on setting up the **ssoadm** command.

Global Options

The following global options are supported.

`--debug, -d`

Run in debug mode. Results sent to the debug file.

`--help, -?`

Print usage.

This command can also be used with subcommands as in **ssoadm *subcommand* --help**.

`--information, -O`

Print basic information about the tool.

`--locale, -l`

Name of the locale to display the results.

`--verbose, -v`

Run in verbose mode. Results sent to standard output.

`--version, -V`

Print the version of this tool.

JVM Properties for ssoadm

You can specifically set the authentication module or chain for administrator logins using two JVM settings. These settings provide more control to select the exact authentication mechanisms to be used when **ssoadm** authenticates administrators in the top-level realm.

To set these properties, manually edit the following two JVM settings in the **ssoadm** or **ssoadm.bat** script.

`org.forgerock.openam.ssoadm.auth.indexType`

Specifies the module or chain-based authentication in the top level realm. If the property is set, OpenAM uses only *that* authentication mechanism.

`org.forgerock.openam.ssoadm.auth.indexName`

Specifies the actual name of the authentication module/chain as controlled by the `indexType` setting. For example, if the `indexType` is set to `module_instance` and `indexName` is set to `LDAP`, then **ssoadm** authenticates using only the LDAP authentication module.

Subcommands: By Category

This section lists subcommands by category. The subsequent section lists subcommands in alphabetical order with a short description.

See **ssoadm *subcommand* --help** for detailed options.

Agent Configuration

- **add-agent-to-grp**
- **agent-remove-props**
- **create-agent**
- **create-agent-grp**
- **delete-agent-grps**
- **delete-agents**
- **list-agent-grp-members**
- **list-agent-grps**
- **list-agents**
- **remove-agent-from-grp**
- **show-agent**
- **show-agent-grp**
- **show-agent-membership**

- **show-agent-types**
- **update-agent**
- **update-agent-grp**

Authentication Service Management

- **add-auth-cfg-entr**
- **create-auth-cfg**
- **create-auth-instance**
- **delete-auth-cfgs**
- **delete-auth-instances**
- **get-auth-cfg-entr**
- **get-auth-instance**
- **list-auth-cfgs**
- **list-auth-instances**
- **register-auth-module**
- **unregister-auth-module**
- **update-auth-cfg-entr**
- **update-auth-cfg-props**
- **update-auth-instance**

Data Store Management

- **add-amsdk-idrepo-plugin**
- **create-datastore**
- **delete-datastores**
- **list-datastore-types**
- **list-datastores**
- **show-datastore**

- **update-datastore**

Entitlements

- **add-app-priv**
- **create-appl**
- **create-appl-type**
- **delete-appl-types**
- **delete-appls**
- **list-appl-types**
- **list-appls**
- **set-appl**
- **set-entitlement-conf**
- **show-app-priv**
- **show-appl**
- **show-entitlement-conf**
- **update-app-priv**
- **update-app-priv-resources**
- **update-app-priv-subjects**

Federation Management

- **add-cot-member**
- **create-cot**
- **create-metadata-templ**
- **delete-cot**
- **delete-entity**
- **do-bulk-federation**
- **export-entity**

- **import-bulk-fed-data**
- **import-entity**
- **list-cot-members**
- **list-cots**
- **list-entities**
- **remove-cot-member**
- **update-entity-keyinfo**

Identity Management

- **add-member**
- **add-privileges**
- **add-svc-identity**
- **create-identity**
- **delete-identities**
- **get-identity**
- **get-identity-svcs**
- **list-identities**
- **list-identity-assignable-svcs**
- **remove-member**
- **remove-privileges**
- **remove-svc-identity**
- **set-identity-attrs**
- **set-identity-svc-attrs**
- **show-identity-ops**
- **show-identity-svc-attrs**
- **show-identity-types**

- **show-members**
- **show-memberships**
- **show-privileges**

Policy Management

- **create-xacml**
- **delete-xacml**
- **list-xacml**

Realm Management

- **add-svc-attrs**
- **add-svc-realm**
- **create-realm**
- **delete-realm**
- **delete-realm-attr**
- **get-realm**
- **get-realm-svc-attrs**
- **list-realm-assignable-svcs**
- **list-realms**
- **remove-svc-attrs**
- **remove-svc-realm**
- **set-realm-attrs**
- **set-svc-attrs**
- **set-realm-svc-attrs**
- **show-auth-modules**
- **show-data-types**
- **show-realm-svcs**

Server Configuration

- **add-site-members**
- **add-site-sec-urls**
- **clone-server**
- **create-server**
- **create-site**
- **delete-server**
- **delete-site**
- **export-server**
- **get-svrcfg-xml**
- **import-server**
- **list-server-cfg**
- **list-servers**
- **list-sites**
- **remove-server-cfg**
- **remove-site-members**
- **remove-site-sec-urls**
- **set-site-pri-url**
- **set-site-sec-urls**
- **set-svrcfg-xml**
- **show-site**
- **show-site-members**
- **update-server-cfg**

Service Management

To translate settings applied in OpenAM console to service attributes for use with **ssoadm**, login to the OpenAM console as as `amadmin` and access the services page, such as `http://openam.example.com:8080/openam/services.jsp`.

- **add-attr-defs**
- **add-attrs**
- **add-plugin-interface**
- **add-sub-schema**
- **create-sub-cfg**
- **create-svc**
- **create-svrcfg-xml**
- **delete-attr**
- **delete-sub-cfg**
- **delete-svc**
- **export-svc-cfg**
- **get-attr-defs**
- **get-revision-number**
- **get-sub-cfg**
- **import-svc-cfg**
- **remove-attr-choicevals**
- **remove-attr-defs**
- **remove-sub-schema**
- **set-attr-any**
- **set-attr-bool-values**
- **set-attr-choicevals**
- **set-attr-defs**
- **set-attr-end-range**
- **set-attr-i18n-key**
- **set-attr-start-range**
- **set-attr-syntax**

- **set-attr-type**
- **set-attr-ui-type**
- **set-attr-validator**
- **set-attr-view-bean-url**
- **set-inheritance**
- **set-plugin-viewbean-url**
- **set-revision-number**
- **set-sub-cfg**
- **set-svc-i18n-key**
- **set-svc-view-bean-url**
- **update-svc**

Other

- **add-res-bundle**
- **do-batch**
- **do-migration70**
- **list-res-bundle**
- **list-sessions**
- **remove-res-bundle**

Subcommands: Alphabetical Order

The following subcommands are supported.

See also **ssoadm *subcommand* --help**.

ssoadm add-agent-to-grp

Add agents to a agent group.

Usage: `ssoadm add-agent-to-grp --options [--global-options]`

Options

`--adminid, -u`

Administrator ID of running the command.

`--agentgroupname, -b`

Name of agent group.

`--agentnames, -s`

Names of agents.

`--password-file, -f`

File name that contains password of administrator.

`--realm, -e`

Name of realm.

ssoadm add-amsdk-idrepo-plugin

Create AMSDK IdRepo Plug-in

Usage: `ssoadm add-amsdk-idrepo-plugin --options [--global-options]`

Options

`--adminid, -u`

Administrator ID of running the command.

`--basedn, -b`

Directory Server base distinguished name.

`--bind-password-file, -m`

File that contains password of bind password.

`--binddn, -e`

Directory Server bind distinguished name.

`--directory-servers, -s`

directory servers <protocol>://<hostname>:<port>. Can have multiple entries.

--dsame-password-file, -x

File that contains password of the dsameuser

--password-file, -f

File name that contains password of administrator.

--puser-password-file, -p

File that contains password of the puser

[--org, -o]

Organization objects naming attribute (defaults to 'o')

[--user, -a]

User objects naming attribute (defaults to 'uid')

ssoadm add-app-priv

Add a policy set privilege to delegate resources of a given policy set. Note that policy sets are cached for 30 minutes. Restart OpenAM to apply changes immediately.

Usage: `ssoadm add-app-priv --options [--global-options]`

Options

--actions, -a

Possible values are READ, MODIFY, DELEGATE, ALL

--adminid, -u

Administrator ID of running the command.

--application, -t

Policy set name

--name, -m

Name for the this delegation

--password-file, -f

File name that contains password of administrator.

--realm, -e

Realm name

--subjects, -s

Subject name

--subjecttype, -b

Possible values are User or Group

[--description, -p]

Description for the this delegation.

[--resources, -r]

Resources to delegate, All resources in the policy set will be delegated if this option is absent.

ssoadm add-attr-defs

Add default attribute values in schema.

Usage: `ssoadm add-attr-defs --options [--global-options]`

Options

--adminid, -u

Administrator ID of running the command.

--password-file, -f

File name that contains password of administrator.

--schematype, -t

Type of schema.

--servicename, -s

Name of service.

[--attributevalues, -a]

Attribute values e.g. homeaddress=here.

[--datafile, -D]

Name of file that contains attribute values data.

[--subschemaname, -c]

Name of sub schema.

ssoadm add-attrs

Add attribute schema to an existing service.

Usage: `ssoadm add-attrs --options [--global-options]`

Options

--adminid, -u

Administrator ID of running the command.

--attributeschemafile, -F

XML file containing attribute schema definition.

--password-file, -f

File name that contains password of administrator.

--schematype, -t

Schema Type.

--servicename, -s

Service Name.

[--subschemaname, -c]

Name of sub schema.

ssoadm add-auth-cfg-entr

Add authentication configuration entry

Usage: `ssoadm add-auth-cfg-entr --options [--global-options]`

Options

--adminid, -u

Administrator ID of running the command.

--criteria, -c

Criteria for this entry. Possible values are REQUIRED, OPTIONAL, SUFFICIENT, REQUISITE

--modulename, -o

Module Name.

--name, -m

Name of authentication configuration.

--password-file, -f

File name that contains password of administrator.

--realm, -e

Name of realm.

[--options, -t]

Options for this entry.

[--position, -p]

Position where the new entry is to be added. This is option is not set, entry shall be added to the end of the list. If value of this option is 0, it will be inserted to the front of the list. If value is greater of the length of the list, entry shall be added to the end of the list.

ssoadm add-cot-member

Add a member to a circle of trust.

Usage: `ssoadm add-cot-member --options [--global-options]`

Options

--adminid, -u

Administrator ID of running the command.

--cot, -t

Circle of Trust

--entityid, -y

Entity ID

--password-file, -f

File name that contains password of administrator.

[--realm, -e]

Realm where circle of trust resides

[--spec, -c]

Specify metadata specification, either wsfed, idff or saml2, defaults to saml2

ssoadm add-member

Add an identity as member of another identity

Usage: `ssoadm add-member --options [--global-options]`

Options

--adminid, -u

Administrator ID of running the command.

--idname, -i

Name of identity.

--idtype, -t

Type of Identity

--memberidname, -m

Name of identity that is member.

--memberidtype, -y

Type of Identity of member such as User, Role and Group.

--password-file, -f

File name that contains password of administrator.

--realm, -e

Name of realm.

ssoadm add-plugin-interface

Add Plug-in interface to service.

Usage: `ssoadm add-plugin-interface --options [--global-options]`

Options

`--adminid, -u`

Administrator ID of running the command.

`--i18nkey, -k`

Plug-in I18n Key.

`--interfacename, -i`

Name of interface.

`--password-file, -f`

File name that contains password of administrator.

`--pluginname, -g`

Name of Plug-in.

`--servicename, -s`

Name of service.

ssoadm add-plugin-schema

Add Plug-in schema to service.

Usage: `ssoadm add-plugin-schema --options [--global-options]`

Options

`--adminid, -u`

Administrator ID of running the command.

`--classname, -c`

Name of the Plugin Schema class implementation

`--i18nkey, -k`

Plug-in I18n Key.

`--i18nname, -n`

Plug-in I18n Name.

--interfacename, -i

Name of interface.

--password-file, -f

File name that contains password of administrator.

--pluginname, -g

Name of Plug-in.

--servicename, -s

Name of service.

ssoadm add-privileges

Add privileges to an identity. To add a privilege to all authenticated users, use the "All Authenticated Users" idname with "role" idtype.

Usage: `ssoadm add-privileges --options [--global-options]`

Options

--adminid, -u

Administrator ID of running the command.

--idname, -i

Name of identity.

--idtype, -t

Type of Identity such as Role and Group.

--password-file, -f

File name that contains password of administrator.

--privileges, -g

Name of privileges to be added. Privilege names are AgentAdmin, ApplicationModifyAccess, ApplicationReadAccess, ApplicationTypesReadAccess, ConditionTypesReadAccess, DecisionCombinersReadAccess, EntitlementRestAccess, FederationAdmin, LogAdmin, LogRead, LogWrite, PolicyAdmin, PrivilegeRestAccess, PrivilegeRestReadAccess, RealmAdmin, RealmReadAccess, ResourceTypeModifyAccess, ResourceTypeReadAccess, SubjectAttributesReadAccess, and SubjectTypesReadAccess.

--realm, -e

Name of realm.

ssoadm add-res-bundle

Add resource bundle to data store.

Usage: `ssoadm add-res-bundle --options [--global-options]`

Options

--adminid, -u

Administrator ID of running the command.

--bundlefilename, -B

Resource bundle physical file name.

--bundlename, -b

Resource Bundle Name.

--password-file, -f

File name that contains password of administrator.

[--bundlelocale, -o]

Locale of the resource bundle.

ssoadm add-site-members

Add members to a site.

Usage: `ssoadm add-site-members --options [--global-options]`

Options

--adminid, -u

Administrator ID of running the command.

--password-file, -f

File name that contains password of administrator.

--servernames, -e

Server names, e.g. http://www.example.com:8080/fam

--sitename, -s

Site name, e.g. mysite

ssoadm add-site-sec-urls

Add Site Secondary URLs.

Usage: `ssoadm add-site-sec-urls --options [--global-options]`

Options

--adminid, -u

Administrator ID of running the command.

--password-file, -f

File name that contains password of administrator.

--secondaryurls, -a

Secondary URLs

--sitename, -s

Site name, e.g. mysite

ssoadm add-sub-schema

Add sub schema.

Usage: `ssoadm add-sub-schema --options [--global-options]`

Options

--adminid, -u

Administrator ID of running the command.

--filename, -F

Name of file that contains the schema

--password-file, -f

File name that contains password of administrator.

--schematype, -t

Type of schema.

--servicename, -s

Name of service.

ssoadm add-svc-attrs

Add service attribute values in a realm. Long content for an attribute can be supplied in a file by appending '-file' to the attribute name, and giving the filename as the value.

Usage: `ssoadm add-svc-attrs --options [--global-options]`

Options

--adminid, -u

Administrator ID of running the command.

--password-file, -f

File name that contains password of administrator.

--realm, -e

Name of realm.

--servicename, -s

Name of service.

[--attributevalues, -a]

Attribute values to be added e.g. homeaddress=here.

[--datafile, -D]

Name of file that contains attribute values to be added.

ssoadm add-svc-identity

Add Service to an identity

Usage: `ssoadm add-svc-identity --options [--global-options]`

Options

`--adminid, -u`

Administrator ID of running the command.

`--idname, -i`

Name of identity.

`--idtype, -t`

Type of Identity such as User, Role and Group.

`--password-file, -f`

File name that contains password of administrator.

`--realm, -e`

Name of realm.

`--servicename, -s`

Name of service.

`[--attributevalues, -a]`

Attribute values e.g. homeaddress=here.

`[--datafile, -D]`

Name of file that contains attribute values data.

ssoadm add-svc-realm

Add service to a realm. Long content for an attribute can be supplied in a file by appending '-file' to the attribute name, and giving the filename as the value.

Usage: `ssoadm add-svc-realm --options [--global-options]`

Options

`--adminid, -u`

Administrator ID of running the command.

--password-file, -f

File name that contains password of administrator.

--realm, -e

Name of realm.

--servicename, -s

Service Name.

[--attributevalues, -a]

Attribute values e.g. homeaddress=here.

[--datafile, -D]

Name of file that contains attribute values data.

ssoadm agent-remove-props

Remove agent's properties.

Usage: `ssoadm agent-remove-props --options [--global-options]`

Options

--adminid, -u

Administrator ID of running the command.

--agentname, -b

Name of agent.

--attributenames, -a

properties name(s).

--password-file, -f

File name that contains password of administrator.

--realm, -e

Name of realm.

ssoadm clone-server

Clone a server instance.

Usage: `ssoadm clone-server --options [--global-options]`

Options

`--adminid, -u`

Administrator ID of running the command.

`--cloneservername, -o`

Clone server name

`--password-file, -f`

File name that contains password of administrator.

`--servername, -s`

Server name

ssoadm create-agent

Create a new agent configuration.

Usage: `ssoadm create-agent --options [--global-options]`

Options

`--adminid, -u`

Administrator ID of running the command.

`--agentname, -b`

Name of agent.

`--agenttype, -t`

Type of agent. Possible values: J2EEAgent, WebAgent, 2.2_Agent, SharedAgent, OAuth2Client

`--password-file, -f`

File name that contains password of administrator.

`--realm, -e`

Name of realm.

[--agenturl, -g]

Agent URL. e.g. http://www.agent.example:8080/agent. WebAgent does not take URL with path. e.g. http://www.agent.example:8080. This option is valid only for J2EEAgent and WebAgent agent types, and is required when the agent type is J2EEAgent or WebAgent.

[--attributevalues, -a]

Properties e.g. sunIdentityServerDeviceKeyValue=https://agent.example.com:443/

[--datafile, -D]

Name of file that contains properties.

[--serverurl, -s]

Server URL. e.g. http://www.example.com:58080/openam. This option is valid only for J2EEAgent and WebAgent agent types, and is required when the agent type is J2EEAgent or WebAgent.

ssoadm create-agent-grp

Create a new agent group.

Usage: `ssoadm create-agent-grp --options [--global-options]`

Options

--adminid, -u

Administrator ID of running the command.

--agentgroupname, -b

Name of agent group.

--agenttype, -t

Type of agent group. e.g. J2EEAgent, WebAgent

--password-file, -f

File name that contains password of administrator.

--realm, -e

Name of realm.

[--attributevalues, -a]

Properties e.g. homeaddress=here.

[--datafile, -D]

Name of file that contains properties.

[--serverurl, -s]

Server URL. e.g. http://www.example.com:58080/openam. This option is valid for J2EEAgent and WebAgent.

ssoadm create-appl

Create policy set.

Usage: `ssoadm create-appl --options [--global-options]`

Options

--adminid, -u

Administrator ID of running the command.

--applicationtype, -t

Application type name

--name, -m

Policy set name

--password-file, -f

File name that contains password of administrator.

--realm, -e

Realm name

[--attributevalues, -a]

Attribute values e.g. applicationType=iPlanetAMWebAgentService.

[--datafile, -D]

Name of file that contains attribute values data. Mandatory attributes are resources, subjects, conditions and entitlementCombiner. Optional ones are actions, searchIndexImpl, saveIndexImpl, resourceComparator, subjectAttributeNames.

ssoadm create-appl-type

Create application type.

Usage: `ssoadm create-appl-type --options [--global-options]`

Options

`--adminid, -u`

Administrator ID of running the command.

`--name, -m`

Application Type name

`--password-file, -f`

File name that contains password of administrator.

`[--attributevalues, -a]`

Application Type attribute values e.g. actions=enabled=true.

`[--datafile, -D]`

Name of file that contains attribute type values data. Mandatory attributes are actions, searchIndexImpl and saveIndexImpl. Optional are resourceComparator.

ssoadm create-auth-cfg

Create authentication configuration

Usage: `ssoadm create-auth-cfg --options [--global-options]`

Options

`--adminid, -u`

Administrator ID of running the command.

`--name, -m`

Name of authentication configuration.

`--password-file, -f`

File name that contains password of administrator.

`--realm, -e`

Name of realm.

ssoadm create-auth-instance

Create authentication module instance

Usage: `ssoadm create-auth-instance --options [--global-options]`

Options

`--adminid, -u`

Administrator ID of running the command.

`--authtype, -t`

Type of authentication module instance. Possible values include AD, Adaptive, Anonymous, Cert, DataStore, DeviceIdMatch, DeviceIdSave, Federation, HOTP, HTTPBasic, JDBC, LDAP, Membership, MSISDN, OATH, OAuth, OpenIdConnect, PersistentCookie, RADIUS, SAE, Scripted, WindowsDesktopSSO, NT, and WSSAuthModule.

`--name, -m`

Name of authentication module instance.

`--password-file, -f`

File name that contains password of administrator.

`--realm, -e`

Name of realm.

ssoadm create-cot

Create circle of trust.

Usage: `ssoadm create-cot --options [--global-options]`

Options

`--adminid, -u`

Administrator ID of running the command.

`--cot, -t`

Circle of Trust

`--password-file, -f`

File name that contains password of administrator.

[--prefix, -p]

Prefix URL for idp discovery reader and writer URL.

[--realm, -e]

Realm where circle of trust resides

[--trustedproviders, -k]

Trusted Providers

ssoadm create-datastore

Create data store under a realm

Usage: `ssoadm create-datastore --options [--global-options]`

Options

--adminid, -u

Administrator ID of running the command.

--datatype, -t

Type of datastore. Use the list-datastore-types subcommand to get a list of supported datastore types.

--name, -m

Name of datastore.

--password-file, -f

File name that contains password of administrator.

--realm, -e

Name of realm.

[--attributevalues, -a]

Attribute values e.g. sunIdRepoClass=com.sun.identity.idm.plugins.files.FilesRepo.

[--datafile, -D]

Name of file that contains attribute values data.

ssoadm create-identity

Create identity in a realm

Usage: `ssoadm create-identity --options [--global-options]`

Options

`--adminid, -u`

Administrator ID of running the command.

`--idname, -i`

Name of identity.

`--idtype, -t`

Type of Identity such as User, Role and Group.

`--password-file, -f`

File name that contains password of administrator.

`--realm, -e`

Name of realm.

`[--attributevalues, -a]`

Attribute values e.g. sunIdentityServerDeviceStatus=Active.

`[--datafile, -D]`

Name of file that contains attribute values data.

ssoadm create-metadata-templ

Create new metadata template.

Usage: `ssoadm create-metadata-templ --options [--global-options]`

Options

`--adminid, -u`

Administrator ID of running the command.

`--entityid, -y`

Entity ID

--password-file, -f

File name that contains password of administrator.

[--affiecertalias, -K]

Affiliation encryption certificate alias

[--affiliation, -F]

Specify metaAlias for hosted affiliation. to be created. The format must be <realm name>/<identifier>

[--affimembers, -M]

Affiliation members

[--affiownerid, -N]

Affiliation Owner ID

[--affiscertalias, -J]

Affiliation signing certificate alias

[--attraecertalias, -G]

Attribute authority encryption certificate alias.

[--attrascertalias, -B]

Attribute authority signing certificate alias

[--attrauthority, -I]

Specify metaAlias for hosted attribute authority to be created. The format must be <realm name>/<identifier>.

[--attrqecertalias, -R]

Attribute query provider encryption certificate alias

[--attrqscertalias, -A]

Attribute query provider signing certificate alias

[--attrqueryprovider, -S]

Specify metaAlias for hosted attribute query provider to be created. The format must be <realm name>/<identifier>.

[--authnaecertalias, -E]

Authentication authority encryption certificate alias.

[--authnascertalias, -D]

Authentication authority signing certificate alias

[--authnauthority, -C]

Specify metaAlias for hosted authentication authority to be created. The format must be <realm name>/<identifier>.

[--extended-data-file, -x]

Specify file name for the extended metadata to be created. XML will be displayed on terminal if this file name is not provided.

[--identityprovider, -i]

Specify metaAlias for hosted identity provider to be created. The format must be <realm name>/<identifier>.

[--idpecertalias, -g]

Identity provider encryption certificate alias.

[--idpscertalias, -b]

Identity provider signing certificate alias

[--meta-data-file, -m]

Specify file name for the standard metadata to be created. XML will be displayed on terminal if this file name is not provided.

[--serviceprovider, -s]

Specify metaAlias for hosted service provider to be created. The format must be <realm name>/<identifier>.

[--specertalias, -r]

Service provider encryption certificate alias

[--spec, -c]

Specify metadata specification, either wsfed, idff or saml2, defaults to saml2

[--spscertalias, -a]

Service provider signing certificate alias

[--xacmlpdpecertalias, -j]

Policy decision point encryption certificate alias

[--xacmlpdpscertalias, -t]

Policy decision point signing certificate alias

[--xacmlpdp, -p]

Specify metaAlias for policy decision point to be created. The format must be <realm name>/<identifier>.

[--xacmlpepecertalias, -z]

Policy enforcement point encryption certificate alias

[--xacmlpepscertalias, -k]

Policy enforcement point signing certificate alias

[--xacmlpep, -e]

Specify metaAlias for policy enforcement point to be created. The format must be <realm name>/<identifier>.

ssoadm create-realm

Create realm.

Usage: `ssoadm create-realm --options [--global-options]`

Options

--adminid, -u

Administrator ID of running the command.

--password-file, -f

File name that contains password of administrator.

--realm, -e

Name of realm to be created.

ssoadm create-server

Create a server instance.

Usage: `ssoadm create-server --options [--global-options]`

Options

`--adminid, -u`

Administrator ID of running the command.

`--password-file, -f`

File name that contains password of administrator.

`--serverconfigxml, -X`

Server Configuration XML file name.

`--servername, -s`

Server name, e.g. http://www.example.com:8080/fam

`[--attributevalues, -a]`

Attribute values e.g. homeaddress=here.

`[--datafile, -D]`

Name of file that contains attribute values data.

ssoadm create-site

Create a site.

Usage: `ssoadm create-site --options [--global-options]`

Options

`--adminid, -u`

Administrator ID of running the command.

`--password-file, -f`

File name that contains password of administrator.

`--sitename, -s`

Site name, e.g. mysite

`--siteurl, -i`

Site's primary URL, e.g. http://www.example.com:8080

[--secondaryurls, -a]

Secondary URLs

ssoadm create-sub-cfg

Create a new sub configuration. Long content for an attribute can be supplied in a file by appending '-file' to the attribute name, and giving the filename as the value.

Usage: `ssoadm create-sub-cfg --options [--global-options]`

Options

--adminid, -u

Administrator ID of running the command.

--password-file, -f

File name that contains password of administrator.

--servicename, -s

Name of service.

--subconfigname, -g

Sub-schema name of (or path to) the type of sub-configuration being added.

[--attributevalues, -a]

Attribute values e.g. homeaddress=here.

[--datafile, -D]

Name of file that contains attribute values data.

[--priority, -p]

Priority of the sub configuration.

[--realm, -e]

Name of realm (Sub Configuration shall be added to global configuration if this option is not provided).

[--subconfigid, -b]

User-specfieid ID of (or path to) the sub-configuration.

ssoadm create-svc

Create a new service in server.

Usage: `ssoadm create-svc --options [--global-options]`

Options

`--adminid, -u`

Administrator ID of running the command.

`--password-file, -f`

File name that contains password of administrator.

`--xmlfile, -X`

XML file(s) that contains schema.

`[--continue, -c]`

Continue adding service if one or more previous service cannot be added.

ssoadm create-svrcfg-xml

Create serverconfig.xml file. No options are required for flat file configuration data store.

Usage: `ssoadm create-svrcfg-xml --options [--global-options]`

Options

`--adminid, -u`

Administrator ID of running the command.

`--password-file, -f`

File name that contains password of administrator.

`[--basedn, -b]`

Directory Server base distinguished name.

`[--dsadmin, -a]`

Directory Server administrator distinguished name

[--dshost, -t]

Directory Server host name

[--dspassword-file, -x]

File that contains Directory Server administrator password

[--dsport, -p]

Directory Server port number

[--outfile, -o]

File name where serverconfig XML is written.

ssoadm create-xacml

Create policies in a realm with XACML input.

Usage: `ssoadm create-xacml --options [--global-options]`

Options

--adminid, -u

Administrator ID of running the command.

--password-file, -f

File name that contains password of administrator.

--realm, -e

Name of realm.

--xmlfile, -X

File that contains the policy XACML definition. In the console, paste the XML into the text field instead.

[--dryrun, -n]

Provide a summary of the policies which would be updated, and those which would be added, as a result of the create-xacml command without the 'dryrun' option specified. Nothing will be updated or added when using this option.

[--outfile, -o]

Filename where the output of a 'dryrun' command will be sent to. If no 'dryrun' command is specified, the outfile will not be used for anything.

ssoadm delete-agent-grps

Delete agent groups.

Usage: `ssoadm delete-agent-grps --options [--global-options]`

Options

`--adminid, -u`

Administrator ID of running the command.

`--password-file, -f`

File name that contains password of administrator.

`--realm, -e`

Name of realm.

`[--agentgroupnames, -s]`

Separate multiple agent group names with spaces.

`[--file, -D]`

File containing agent group names, with multiple group names separated by spaces.

ssoadm delete-agents

Delete agent configurations.

Usage: `ssoadm delete-agents --options [--global-options]`

Options

`--adminid, -u`

Administrator ID of running the command.

`--password-file, -f`

File name that contains password of administrator.

`--realm, -e`

Name of realm.

`[--agentnames, -s]`

Separate multiple agent names with spaces.

[--file, -D]

File containing agent names, with multiple agent names separated by spaces.

ssoadm delete-appl-types

Delete application types.

Usage: `ssoadm delete-appl-types --options [--global-options]`

Options

--adminid, -u

Administrator ID of running the command.

--names, -m

Application Type names

--password-file, -f

File name that contains password of administrator.

ssoadm delete-appls

Delete policy sets. Note that policy sets are cached for 30 minutes. Restart OpenAM to apply changes immediately.

Usage: `ssoadm delete-appls --options [--global-options]`

Options

--adminid, -u

Administrator ID of running the command.

--names, -m

Policy set names

--password-file, -f

File name that contains password of administrator.

--realm, -e

Realm name

ssoadm delete-attr

Delete attribute schemas from a service

Usage: `ssoadm delete-attr --options [--global-options]`

Options

`--adminid, -u`

Administrator ID of running the command.

`--attributeschema, -a`

Name of attribute schema to be removed.

`--password-file, -f`

File name that contains password of administrator.

`--schematype, -t`

Type of schema.

`--servicename, -s`

Name of service.

`[--subschemaname, -c]`

Name of sub schema.

ssoadm delete-attr-def-values

Delete attribute schema default values.

Usage: `ssoadm delete-attr-def-values --options [--global-options]`

Options

`--adminid, -u`

Administrator ID of running the command.

`--attributeschema, -a`

Name of attribute schema

--defaultvalues, -e

Default value(s) to be deleted

--password-file, -f

File name that contains password of administrator.

--schematype, -t

Type of schema.

--servicename, -s

Name of service.

[--subschemaname, -c]

Name of sub schema.

ssoadm delete-auth-cfgs

Delete authentication configurations

Usage: `ssoadm delete-auth-cfgs --options [--global-options]`

Options

--adminid, -u

Administrator ID of running the command.

--names, -m

Name of authentication configurations.

--password-file, -f

File name that contains password of administrator.

--realm, -e

Name of realm.

ssoadm delete-auth-instances

Delete authentication instances

Usage: `ssoadm delete-auth-instances --options [--global-options]`

Options

`--adminid, -u`

Administrator ID of running the command.

`--names, -m`

Name of authentication instances.

`--password-file, -f`

File name that contains password of administrator.

`--realm, -e`

Name of realm.

ssoadm delete-cot

Delete circle of trust.

Usage: `ssoadm delete-cot --options [--global-options]`

Options

`--adminid, -u`

Administrator ID of running the command.

`--cot, -t`

Circle of Trust

`--password-file, -f`

File name that contains password of administrator.

`[--realm, -e]`

Realm where circle of trust resides

ssoadm delete-datastores

Delete data stores under a realm

Usage: `ssoadm delete-datastores --options [--global-options]`

Options

`--adminid, -u`

Administrator ID of running the command.

`--names, -m`

Names of datastore.

`--password-file, -f`

File name that contains password of administrator.

`--realm, -e`

Name of realm.

ssoadm delete-entity

Delete entity.

Usage: `ssoadm delete-entity --options [--global-options]`

Options

`--adminid, -u`

Administrator ID of running the command.

`--entityid, -y`

Entity ID

`--password-file, -f`

File name that contains password of administrator.

`[--extendedonly, -x]`

Set to flag to delete only extended data.

`[--realm, -e]`

Realm where data resides

`[--spec, -c]`

Specify metadata specification, either wsfed, idff or saml2, defaults to saml2

ssoadm delete-identities

Delete identities in a realm

Usage: `ssoadm delete-identities --options [--global-options]`

Options

`--adminid, -u`

Administrator ID of running the command.

`--idtype, -t`

Type of Identity such as User, Role and Group.

`--password-file, -f`

File name that contains password of administrator.

`--realm, -e`

Name of realm.

`[--file, -D]`

Name of file that contains the identity names to be deleted.

`[--idnames, -i]`

Names of identites.

ssoadm delete-realm

Delete realm.

Usage: `ssoadm delete-realm --options [--global-options]`

Options

`--adminid, -u`

Administrator ID of running the command.

`--password-file, -f`

File name that contains password of administrator.

--realm, -e

Name of realm to be deleted.

[--recursive, -r]

Delete descendent realms recursively.

ssoadm delete-realm-attr

Delete attribute from a realm.

Usage: `ssoadm delete-realm-attr --options [--global-options]`

Options

--adminid, -u

Administrator ID of running the command.

--attributename, -a

Name of attribute to be removed.

--password-file, -f

File name that contains password of administrator.

--realm, -e

Name of realm.

--servicename, -s

Name of service.

ssoadm delete-server

Delete a server instance.

Usage: `ssoadm delete-server --options [--global-options]`

Options

--adminid, -u

Administrator ID of running the command.

--password-file, -f

File name that contains password of administrator.

--servername, -s

Server name, e.g. http://www.example.com:8080/fam

ssoadm delete-site

Delete a site.

Usage: `ssoadm delete-site --options [--global-options]`

Options

--adminid, -u

Administrator ID of running the command.

--password-file, -f

File name that contains password of administrator.

--sitename, -s

Site name, e.g. mysite

ssoadm delete-sub-cfg

Remove Sub Configuration.

Usage: `ssoadm delete-sub-cfg --options [--global-options]`

Options

--adminid, -u

Administrator ID of running the command.

--password-file, -f

File name that contains password of administrator.

--servicename, -s

Name of service.

--subconfigname, -g

Name of sub configuration.

[--realm, -e]

Name of realm (Sub Configuration shall be deleted from the global configuration if this option is not provided).

ssoadm delete-svc

Delete service from the server.

Usage: `ssoadm delete-svc --options [--global-options]`

Options

--adminid, -u

Administrator ID of running the command.

--password-file, -f

File name that contains password of administrator.

--servicename, -s

Service Name(s).

[--continue, -c]

Continue deleting service if one or more previous services cannot be deleted.

[--deletepolicyrule, -r]

Delete policy rule.

ssoadm delete-xacml

Delete XACML policies from a realm.

Usage: `ssoadm delete-xacml --options [--global-options]`

Options

--adminid, -u

Administrator ID of running the command.

--password-file, -f

File name that contains password of administrator.

--realm, -e

Name of realm.

[--file, -D]

Name of file that contains the policy names to be deleted.

[--policynames, -p]

Names of policy to be deleted.

ssoadm do-batch

Do multiple requests in one command.

Usage: `ssoadm do-batch --options [--global-options]`

Options

--adminid, -u

Administrator ID of running the command.

--batchfile, -Z

Name of file that contains commands and options.

--password-file, -f

File name that contains password of administrator.

[--batchstatus, -b]

Name of status file.

[--continue, -c]

Continue processing the rest of the request when preceeding request was erroneous.

ssoadm do-bulk-federation

Perform bulk federation.

Usage: `ssoadm do-bulk-federation --options [--global-options]`

Options

`--adminid, -u`

Administrator ID of running the command.

`--metaalias, -m`

Specify metaAlias for local provider.

`--nameidmapping, -e`

Name of file that will be created by this sub command. It contains remote user Id to name identifier. It shall be used by remote provider to update user profile.

`--password-file, -f`

File name that contains password of administrator.

`--remoteentityid, -r`

Remote entity Id

`--useridmapping, -g`

File name of local to remote user Id mapping. Format <local-user-id>|<remote-user-id>

`[--spec, -c]`

Specify metadata specification, either idff or saml2, defaults to saml2

ssoadm do-migration70

Migrate organization to realm.

Usage: `ssoadm do-migration70 --options [--global-options]`

Options

`--adminid, -u`

Administrator ID of running the command.

`--entrydn, -e`

Distinguished name of organization to be migrated.

`--password-file, -f`

File name that contains password of administrator.

ssoadm embedded-status

Status of embedded store.

Usage: `ssoadm embedded-status --options [--global-options]`

Options

`--adminid, -u`

Administrator ID of running the command.

`--password-file, -f`

File name that contains password of administrator.

`--port, -p`

Embedded store port

`[--password, -w]`

Embedded store password

ssoadm export-entity

Export entity.

Usage: `ssoadm export-entity --options [--global-options]`

Options

`--adminid, -u`

Administrator ID of running the command.

`--entityid, -y`

Entity ID

`--password-file, -f`

File name that contains password of administrator.

`[--extended-data-file, -x]`

Extended data

`[--meta-data-file, -m]`

Metadata

[--realm, -e]

Realm where data resides

[--sign, -g]

Set this flag to sign the metadata

[--spec, -c]

Specify metadata specification, either wsfed, idff or saml2, defaults to saml2

ssoadm export-server

Export a server instance.

Usage: `ssoadm export-server --options [--global-options]`

Options

--adminid, -u

Administrator ID of running the command.

--password-file, -f

File name that contains password of administrator.

--servername, -s

Server name

[--outfile, -o]

Filename where configuration was written.

ssoadm export-svc-cfg

Export service configuration. In production environments, you should back up the service configuration using file system utilities or the export-ldif command. Note that export-ldif/import-ldif commands must be on the same deployment where the encryption keys are located.

Usage: `ssoadm export-svc-cfg --options [--global-options]`

Options

--adminid, -u

Administrator ID of running the command.

--encryptsecret, -e

Secret key for encrypting password. Any arbitrary value can be specified.

--password-file, -f

File name that contains password of administrator.

[--outfile, -o]

Filename where configuration was written.

ssoadm get-attr-choicevals

Get choice values of attribute schema.

Usage: `ssoadm get-attr-choicevals --options [--global-options]`

Options

--adminid, -u

Administrator ID of running the command.

--attributename, -a

Name of attribute.

--password-file, -f

File name that contains password of administrator.

--schematype, -t

Type of schema.

--servicename, -s

Name of service.

[--subschemaname, -c]

Name of sub schema.

ssoadm get-attr-defs

Get default attribute values in schema.

Usage: `ssoadm get-attr-defs --options [--global-options]`

Options

`--adminid, -u`

Administrator ID of running the command.

`--password-file, -f`

File name that contains password of administrator.

`--schematype, -t`

Type of schema. One of dynamic, global, or organization (meaning realm).

`--servicename, -s`

Name of service.

`[--attributenames, -a]`

Attribute name(s).

`[--subschemaname, -c]`

Name of sub schema.

ssoadm get-auth-cfg-entr

Get authentication configuration entries

Usage: `ssoadm get-auth-cfg-entr --options [--global-options]`

Options

`--adminid, -u`

Administrator ID of running the command.

`--name, -m`

Name of authentication configuration.

`--password-file, -f`

File name that contains password of administrator.

`--realm, -e`

Name of realm.

ssoadm get-auth-instance

Get authentication instance values

Usage: `ssoadm get-auth-instance --options [--global-options]`

Options

`--adminid, -u`

Administrator ID of running the command.

`--name, -m`

Name of authentication instance.

`--password-file, -f`

File name that contains password of administrator.

`--realm, -e`

Name of realm.

ssoadm get-identity

Get identity property values

Usage: `ssoadm get-identity --options [--global-options]`

Options

`--adminid, -u`

Administrator ID of running the command.

`--idname, -i`

Name of identity.

`--idtype, -t`

Type of Identity such as User, Role and Group.

`--password-file, -f`

File name that contains password of administrator.

--realm, -e

Name of realm.

[--attributenames, -a]

Attribute name(s). All attribute values shall be returned if the option is not provided.

ssoadm get-identity-svcs

Get the service in an identity

Usage: `ssoadm get-identity-svcs --options [--global-options]`

Options

--adminid, -u

Administrator ID of running the command.

--idname, -i

Name of identity.

--idtype, -t

Type of Identity such as User, Role and Group.

--password-file, -f

File name that contains password of administrator.

--realm, -e

Name of realm.

ssoadm get-realm

Get realm property values.

Usage: `ssoadm get-realm --options [--global-options]`

Options

--adminid, -u

Administrator ID of running the command.

--password-file, -f

File name that contains password of administrator.

--realm, -e

Name of realm.

--servicename, -s

Name of service.

ssoadm get-realm-svc-attrs

Get realm's service attribute values.

Usage: `ssoadm get-realm-svc-attrs --options [--global-options]`

Options

--adminid, -u

Administrator ID of running the command.

--password-file, -f

File name that contains password of administrator.

--realm, -e

Name of realm.

--servicename, -s

Name of service.

ssoadm get-recording-status

Get the status of recording operations.

Usage: `ssoadm get-recording-status --options [--global-options]`

Options

--adminid, -u

Administrator ID of running the command.

--password-file, -f

File name that contains password of administrator.

--servername, -s

Server name, e.g. http://openam.example.com:8080/openam

ssoadm get-revision-number

Get service schema revision number.

Usage: `ssoadm get-revision-number --options [--global-options]`

Options

--adminid, -u

Administrator ID of running the command.

--password-file, -f

File name that contains password of administrator.

--servicename, -s

Name of service.

ssoadm get-sub-cfg

Get sub configuration.

Usage: `ssoadm get-sub-cfg --options [--global-options]`

Options

--adminid, -u

Administrator ID of running the command.

--password-file, -f

File name that contains password of administrator.

--servicename, -s

Name of service.

--subconfigname, -g

Name of sub configuration.

[--realm, -e]

Name of realm (Sub Configuration shall be retrieved from the global configuration if this option is not provided).

ssoadm get-svrcfg-xml

Get server configuration XML from centralized data store

Usage: `ssoadm get-svrcfg-xml --options [--global-options]`

Options

--adminid, -u

Administrator ID of running the command.

--password-file, -f

File name that contains password of administrator.

--servername, -s

Server name, e.g. http://www.example.com:8080/fam

[--outfile, -o]

File name where serverconfig XML is written.

ssoadm import-bulk-fed-data

Import bulk federation data which is generated by 'do-bulk-federation' sub command.

Usage: `ssoadm import-bulk-fed-data --options [--global-options]`

Options

--adminid, -u

Administrator ID of running the command.

--bulk-data-file, -g

File name of bulk federation data which is generated by 'do-bulk-federation' sub command.

--metaalias, -m

Specify metaAlias for local provider.

--password-file, -f

File name that contains password of administrator.

[--spec, -c]

Specify metadata specification, either idff or saml2, defaults to saml2

ssoadm import-entity

Import entity.

Usage: `ssoadm import-entity --options [--global-options]`

Options

--adminid, -u

Administrator ID of running the command.

--password-file, -f

File name that contains password of administrator.

[--cot, -t]

Specify name of the Circle of Trust this entity belongs.

[--extended-data-file, -x]

Specify file name for the extended entity configuration to be imported.<web>Extended entity configuration to be imported.

[--meta-data-file, -m]

Specify file name for the standard metadata to be imported.<web>Standard metadata to be imported.

[--realm, -e]

Realm where entity resides.

[--spec, -c]

Specify metadata specification, either wsfed, idff or saml2, defaults to saml2

ssoadm import-server

Import a server instance.

Usage: `ssoadm import-server --options [--global-options]`

Options

`--adminid, -u`

Administrator ID of running the command.

`--password-file, -f`

File name that contains password of administrator.

`--servername, -s`

Server name

`--xmlfile, -X`

XML file that contains configuration.

ssoadm import-svc-cfg

Import service configuration. In production environments, you should restore the service configuration using file system utilities or the import-ldif command. Note that import-ldif/export-ldif commands must be on the same deployment where the encryption keys are located.

Usage: `ssoadm import-svc-cfg --options [--global-options]`

Options

`--adminid, -u`

Administrator ID of running the command.

`--encryptsecret, -e`

Secret key for decrypting password.

`--password-file, -f`

File name that contains password of administrator.

`--xmlfile, -X`

XML file that contains configuration data.

ssoadm list-agent-grp-members

List agents in agent group.

Usage: `ssoadm list-agent-grp-members --options [--global-options]`

Options

`--adminid, -u`

Administrator ID of running the command.

`--agentgroupname, -b`

Name of agent group.

`--password-file, -f`

File name that contains password of administrator.

`--realm, -e`

Name of realm.

`[--filter, -x]`

Filter (Pattern).

ssoadm list-agent-grps

List agent groups.

Usage: `ssoadm list-agent-grps --options [--global-options]`

Options

`--adminid, -u`

Administrator ID of running the command.

`--password-file, -f`

File name that contains password of administrator.

`--realm, -e`

Name of realm.

[--agenttype, -t]

Type of agent. e.g. J2EEAgent, WebAgent

[--filter, -x]

Filter (Pattern).

ssoadm list-agents

List agent configurations.

Usage: `ssoadm list-agents --options [--global-options]`

Options

--adminid, -u

Administrator ID of running the command.

--password-file, -f

File name that contains password of administrator.

--realm, -e

Name of realm.

[--agenttype, -t]

Type of agent. e.g. J2EEAgent, WebAgent

[--filter, -x]

Filter (Pattern).

ssoadm list-app-privs

List policy set privileges in a realm.

Usage: `ssoadm list-app-privs --options [--global-options]`

Options

--adminid, -u

Administrator ID of running the command.

--password-file, -f

File name that contains password of administrator.

--realm, -e

Realm name

ssoadm list-appl-types

List application types.

Usage: `ssoadm list-appl-types --options [--global-options]`

Options

--adminid, -u

Administrator ID of running the command.

--password-file, -f

File name that contains password of administrator.

ssoadm list-appls

List policy set in a realm.

Usage: `ssoadm list-appls --options [--global-options]`

Options

--adminid, -u

Administrator ID of running the command.

--password-file, -f

File name that contains password of administrator.

--realm, -e

Realm name

ssoadm list-auth-cfgs

List authentication configurations

Usage: `ssoadm list-auth-cfgs --options [--global-options]`

Options

`--adminid, -u`

Administrator ID of running the command.

`--password-file, -f`

File name that contains password of administrator.

`--realm, -e`

Name of realm.

ssoadm list-auth-instances

List authentication instances

Usage: `ssoadm list-auth-instances --options [--global-options]`

Options

`--adminid, -u`

Administrator ID of running the command.

`--password-file, -f`

File name that contains password of administrator.

`--realm, -e`

Name of realm.

ssoadm list-cot-members

List the members in a circle of trust.

Usage: `ssoadm list-cot-members --options [--global-options]`

Options

`--adminid, -u`

Administrator ID of running the command.

--cot, -t

Circle of Trust

--password-file, -f

File name that contains password of administrator.

[--realm, -e]

Realm where circle of trust resides

[--spec, -c]

Specify metadata specification, either wsfed, idff or saml2, defaults to saml2

ssoadm list-cots

List circles of trust.

Usage: `ssoadm list-cots --options [--global-options]`

Options

--adminid, -u

Administrator ID of running the command.

--password-file, -f

File name that contains password of administrator.

[--realm, -e]

Realm where circle of trusts reside

ssoadm list-datastore-types

List the supported data store types

Usage: `ssoadm list-datastore-types --options [--global-options]`

Options

--adminid, -u

Administrator ID of running the command.

--password-file, -f

File name that contains password of administrator.

ssoadm list-datastores

List data stores under a realm

Usage: `ssoadm list-datastores --options [--global-options]`

Options

--adminid, -u

Administrator ID of running the command.

--password-file, -f

File name that contains password of administrator.

--realm, -e

Name of realm.

ssoadm list-entities

List entities under a realm.

Usage: `ssoadm list-entities --options [--global-options]`

Options

--adminid, -u

Administrator ID of running the command.

--password-file, -f

File name that contains password of administrator.

[--realm, -e]

Realm where entities reside.

[--spec, -c]

Specify metadata specification, either wsfed, idff or saml2, defaults to saml2

ssoadm list-identities

List identities in a realm

Usage: `ssoadm list-identities --options [--global-options]`

Options

`--adminid, -u`

Administrator ID of running the command.

`--filter, -x`

Filter (Pattern).

`--idtype, -t`

Type of Identity such as User, Role and Group.

`--password-file, -f`

File name that contains password of administrator.

`--realm, -e`

Name of realm.

ssoadm list-identity-assignable-svcs

List the assignable service to an identity

Usage: `ssoadm list-identity-assignable-svcs --options [--global-options]`

Options

`--adminid, -u`

Administrator ID of running the command.

`--idname, -i`

Name of identity.

`--idtype, -t`

Type of Identity such as User, Role and Group.

--password-file, -f

File name that contains password of administrator.

--realm, -e

Name of realm.

ssoadm list-realm-assignable-svcs

List the assignable services to a realm.

Usage: `ssoadm list-realm-assignable-svcs --options [--global-options]`

Options

--adminid, -u

Administrator ID of running the command.

--password-file, -f

File name that contains password of administrator.

--realm, -e

Name of realm.

ssoadm list-realms

List realms by name.

Usage: `ssoadm list-realms --options [--global-options]`

Options

--adminid, -u

Administrator ID of running the command.

--password-file, -f

File name that contains password of administrator.

--realm, -e

Name of realm where search begins.

[--filter, -x]

Filter (Pattern).

[--recursive, -r]

Search recursively

ssoadm list-res-bundle

List resource bundle in data store.

Usage: `ssoadm list-res-bundle --options [--global-options]`

Options

--adminid, -u

Administrator ID of running the command.

--bundlename, -b

Resource Bundle Name.

--password-file, -f

File name that contains password of administrator.

[--bundlelocale, -o]

Locale of the resource bundle.

ssoadm list-server-cfg

List server configuration.

Usage: `ssoadm list-server-cfg --options [--global-options]`

Options

--adminid, -u

Administrator ID of running the command.

--password-file, -f

File name that contains password of administrator.

--servername, -s

Server name, e.g. http://www.example.com:8080/fam or enter default to list default server configuration.

[--withdefaults, -w]

Set this flag to get default configuration.

ssoadm list-servers

List all server instances.

Usage: `ssoadm list-servers --options [--global-options]`

Options

--adminid, -u

Administrator ID of running the command.

--password-file, -f

File name that contains password of administrator.

ssoadm list-sessions

List stateful sessions.

Usage: `ssoadm list-sessions --options [--global-options]`

Options

--adminid, -u

Administrator ID of running the command.

--host, -t

Host Name.

--password-file, -f

File name that contains password of administrator.

[--filter, -x]

Filter (Pattern).

[--quiet, -q]

Do not prompt for session invalidation.

ssoadm list-sites

List all sites.

Usage: `ssoadm list-sites --options [--global-options]`

Options

--adminid, -u

Administrator ID of running the command.

--password-file, -f

File name that contains password of administrator.

ssoadm list-xacml

Export policies in realm as XACML.

Usage: `ssoadm list-xacml --options [--global-options]`

Options

--adminid, -u

Administrator ID of running the command.

--password-file, -f

File name that contains password of administrator.

--realm, -e

Name of realm.

[--namesonly, -n]

Returns only names of matching policies. Policies are not returned.

[--outfile, -o]

Filename where policy definition will be printed to. Definition will be printed in standard output if this option is not provided.

[--policynames, -p]

Names of policy. This can be a wildcard. All policy definition in the realm will be returned if this option is not provided.

ssoadm policy-export

Export policy configuration for a given realm

Usage: `ssoadm policy-export --options [--global-options]`

Options

--adminid, -u

Administrator ID of running the command.

--jsonfile, -J

JSON file for which to write the policy model to.

--password-file, -f

File name that contains password of administrator.

--realm, -e

Realm name

--servername, -s

Server name, e.g. http://openam.example.com:8080/openam

ssoadm policy-import

Import policy model into a given realm

Usage: `ssoadm policy-import --options [--global-options]`

Options

--adminid, -u

Administrator ID of running the command.

--jsonfile, -J

JSON file containing the policy model to be imported.

--password-file, -f

File name that contains password of administrator.

--realm, -e

Realm name

--servername, -s

Server name, e.g. http://openam.example.com:8080/openam

ssoadm register-auth-module

Registers authentication module.

Usage: `ssoadm register-auth-module --options [--global-options]`

Options

--adminid, -u

Administrator ID of running the command.

--authmodule, -a

Java class name of authentication module.

--password-file, -f

File name that contains password of administrator.

ssoadm remove-agent-from-grp

Remove agents from a agent group.

Usage: `ssoadm remove-agent-from-grp --options [--global-options]`

Options

--adminid, -u

Administrator ID of running the command.

--agentgroupname, -b

Name of agent group.

--agentnames, -s

Names of agents.

--password-file, -f

File name that contains password of administrator.

--realm, -e

Name of realm.

ssoadm remove-app-priv-resources

Remove policy set privilege resources. Note that policy sets are cached for 30 minutes. Restart OpenAM to apply changes immediately.

Usage: `ssoadm remove-app-priv-resources --options [--global-options]`

Options

--adminid, -u

Administrator ID of running the command.

--application, -t

Policy set name

--name, -m

Name for the this delegation

--password-file, -f

File name that contains password of administrator.

--realm, -e

Realm name

[--resources, -r]

Resources to removed, All resources in the policy set will be removed if this option is absent.

ssoadm remove-app-priv-subjects

Remove policy set privilege subjects.

Usage: `ssoadm remove-app-priv-subjects --options [--global-options]`

Options

`--adminid, -u`

Administrator ID of running the command.

`--name, -m`

Name for the this delegation

`--password-file, -f`

File name that contains password of administrator.

`--realm, -e`

Realm name

`--subjects, -s`

Subject name

`--subjecttype, -b`

Possible values are User or Group

ssoadm remove-app-privs

Remove policy set privileges.

Usage: `ssoadm remove-app-privs --options [--global-options]`

Options

`--adminid, -u`

Administrator ID of running the command.

`--names, -m`

Names of policy set privileges to be removed

`--password-file, -f`

File name that contains password of administrator.

`--realm, -e`

Realm name

ssoadm remove-attr-choicevals

Remove choice values from attribute schema.

Usage: `ssoadm remove-attr-choicevals --options [--global-options]`

Options

`--adminid, -u`

Administrator ID of running the command.

`--attributename, -a`

Name of attribute.

`--choicevalues, -k`

Choice values e.g. Inactive

`--password-file, -f`

File name that contains password of administrator.

`--schematype, -t`

Type of schema.

`--servicename, -s`

Name of service.

`[--subschemaname, -c]`

Name of sub schema.

ssoadm remove-attr-defs

Remove default attribute values in schema.

Usage: `ssoadm remove-attr-defs --options [--global-options]`

Options

`--adminid, -u`

Administrator ID of running the command.

--attributenames, -a

Attribute name(s).

--password-file, -f

File name that contains password of administrator.

--schematype, -t

Type of schema.

--servicename, -s

Name of service.

[--subschemaname, -c]

Name of sub schema.

ssoadm remove-cot-member

Remove a member from a circle of trust.

Usage: `ssoadm remove-cot-member --options [--global-options]`

Options

--adminid, -u

Administrator ID of running the command.

--cot, -t

Circle of Trust

--entityid, -y

Entity ID

--password-file, -f

File name that contains password of administrator.

[--realm, -e]

Realm where circle of trust resides

[--spec, -c]

Specify metadata specification, either wsfed, idff or saml2, defaults to saml2

ssoadm remove-member

Remove membership of identity from another identity

Usage: `ssoadm remove-member --options [--global-options]`

Options

`--adminid, -u`

Administrator ID of running the command.

`--idname, -i`

Name of identity.

`--idtype, -t`

Type of Identity

`--memberidname, -m`

Name of identity that is member.

`--memberidtype, -y`

Type of Identity of member such as User, Role and Group.

`--password-file, -f`

File name that contains password of administrator.

`--realm, -e`

Name of realm.

ssoadm remove-plugin-schema

Add Plug-in interface to service.

Usage: `ssoadm remove-plugin-schema --options [--global-options]`

Options

`--adminid, -u`

Administrator ID of running the command.

--interfacename, -i

Name of interface.

--password-file, -f

File name that contains password of administrator.

--pluginname, -g

Name of Plug-in.

--servicename, -s

Name of service.

ssoadm remove-privileges

Remove privileges from an identity

Usage: `ssoadm remove-privileges --options [--global-options]`

Options

--adminid, -u

Administrator ID of running the command.

--idname, -i

Name of identity.

--idtype, -t

Type of Identity such as Role and Group.

--password-file, -f

File name that contains password of administrator.

--privileges, -g

Name of privileges to be removed. Privilege names are AgentAdmin, ApplicationModifyAccess, ApplicationReadAccess, ApplicationTypesReadAccess, ConditionTypesReadAccess, DecisionCombinersReadAccess, EntitlementRestAccess, FederationAdmin, LogAdmin, LogRead, LogWrite, PolicyAdmin, PrivilegeRestAccess, PrivilegeRestReadAccess, RealmAdmin, RealmReadAccess, ResourceTypeModifyAccess, ResourceTypeReadAccess, SubjectAttributesReadAccess, and SubjectTypesReadAccess.

--realm, -e

Name of realm.

ssoadm remove-res-bundle

Remove resource bundle from data store.

Usage: `ssoadm remove-res-bundle --options [--global-options]`

Options

--adminid, -u

Administrator ID of running the command.

--bundlename, -b

Resource Bundle Name.

--password-file, -f

File name that contains password of administrator.

[--bundlelocale, -o]

Locale of the resource bundle.

ssoadm remove-server-cfg

Remove server configuration.

Usage: `ssoadm remove-server-cfg --options [--global-options]`

Options

--adminid, -u

Administrator ID of running the command.

--password-file, -f

File name that contains password of administrator.

--propertynames, -a

Name of properties to be removed.

--servername, -s

Server name, e.g. http://www.example.com:8080/fam or enter default to remove default server configuration.

ssoadm remove-site-members

Remove members from a site.

Usage: `ssoadm remove-site-members --options [--global-options]`

Options

--adminid, -u

Administrator ID of running the command.

--password-file, -f

File name that contains password of administrator.

--servernames, -e

Server names, e.g. http://www.example.com:8080/fam

--sitename, -s

Site name, e.g. mysite

ssoadm remove-site-sec-urls

Remove Site Secondary URLs.

Usage: `ssoadm remove-site-sec-urls --options [--global-options]`

Options

--adminid, -u

Administrator ID of running the command.

--password-file, -f

File name that contains password of administrator.

--secondaryurls, -a

Secondary URLs

--sitename, -s

Site name, e.g. mysite

ssoadm remove-sub-schema

Remove sub schema.

Usage: `ssoadm remove-sub-schema --options [--global-options]`

Options

--adminid, -u

Administrator ID of running the command.

--password-file, -f

File name that contains password of administrator.

--schematype, -t

Type of schema.

--servicename, -s

Name of service.

--subschemanames, -a

Name(s) of sub schema to be removed.

[--subschemaname, -c]

Name of parent sub schema.

ssoadm remove-svc-attrs

Remove service attribute values in a realm.

Usage: `ssoadm remove-svc-attrs --options [--global-options]`

Options

--adminid, -u

Administrator ID of running the command.

--password-file, -f

File name that contains password of administrator.

--realm, -e

Name of realm.

--servicename, -s

Name of service.

[--attributevalues, -a]

Attribute values to be removed e.g. homeaddress=here.

[--datafile, -D]

Name of file that contains attribute values to be removed.

ssoadm remove-svc-identity

Remove Service from an identity

Usage: `ssoadm remove-svc-identity --options [--global-options]`

Options

--adminid, -u

Administrator ID of running the command.

--idname, -i

Name of identity.

--idtype, -t

Type of Identity such as User, Role and Group.

--password-file, -f

File name that contains password of administrator.

--realm, -e

Name of realm.

--servicename, -s

Name of service.

ssoadm remove-svc-realm

Remove service from a realm.

Usage: `ssoadm remove-svc-realm --options [--global-options]`

Options

`--adminid, -u`

Administrator ID of running the command.

`--password-file, -f`

File name that contains password of administrator.

`--realm, -e`

Name of realm.

`--servicename, -s`

Name of service to be removed.

ssoadm set-appl

Set policy set attributes. Note that policy sets are cached for 30 minutes. Restart OpenAM to apply changes immediately.

Usage: `ssoadm set-appl --options [--global-options]`

Options

`--adminid, -u`

Administrator ID of running the command.

`--name, -m`

Policy set name

`--password-file, -f`

File name that contains password of administrator.

`--realm, -e`

Realm name

[--attributevalues, -a]

Attribute values e.g. applicationType=iPlanetAMWebAgentService.

[--datafile, -D]

Name of file that contains attribute values data. Possible attributes are resources, subjects, conditions, actions, searchIndexImpl, saveIndexImpl, resourceComparator, subjectAttributeNames and entitlementCombiner.

ssoadm set-attr-any

Set any member of attribute schema.

Usage: `ssoadm set-attr-any --options [--global-options]`

Options

--adminid, -u

Administrator ID of running the command.

--any, -y

Attribute Schema Any value

--attributeschema, -a

Name of attribute schema

--password-file, -f

File name that contains password of administrator.

--schematype, -t

Type of schema.

--servicename, -s

Name of service.

[--subschemaname, -c]

Name of sub schema.

ssoadm set-attr-bool-values

Set boolean values of attribute schema.

Usage: `ssoadm set-attr-bool-values --options [--global-options]`

Options

`--adminid, -u`

Administrator ID of running the command.

`--attributename, -a`

Name of attribute.

`--falsei18nkey, -j`

Internationalization key for false value.

`--falsevalue, -z`

Value for false.

`--password-file, -f`

File name that contains password of administrator.

`--schematype, -t`

Type of schema.

`--servicename, -s`

Name of service.

`--truei18nkey, -k`

Internationalization key for true value.

`--truevalue, -e`

Value for true.

`[--subschemaname, -c]`

Name of sub schema.

ssoadm set-attr-choicevals

Set choice values of attribute schema.

Usage: `ssoadm set-attr-choicevals --options [--global-options]`

Options

`--adminid, -u`

Administrator ID of running the command.

`--attributename, -a`

Name of attribute.

`--password-file, -f`

File name that contains password of administrator.

`--schematype, -t`

Type of schema.

`--servicename, -s`

Name of service.

`[--add, -p]`

Set this flag to append the choice values to existing ones.

`[--choicevalues, -k]`

Choice value e.g. o102=Inactive.

`[--datafile, -D]`

Name of file that contains attribute values data.

`[--subschemaname, -c]`

Name of sub schema.

ssoadm set-attr-defs

Set default attribute values in schema.

Usage: `ssoadm set-attr-defs --options [--global-options]`

Options

`--adminid, -u`

Administrator ID of running the command.

--password-file, -f

File name that contains password of administrator.

--schematype, -t

Type of schema.

--servicename, -s

Name of service.

[--attributevalues, -a]

Attribute values e.g. homeaddress=here.

[--datafile, -D]

Name of file that contains attribute values data.

[--subschemaname, -c]

Name of sub schema.

ssoadm set-attr-end-range

Set attribute schema end range.

Usage: `ssoadm set-attr-end-range --options [--global-options]`

Options

--adminid, -u

Administrator ID of running the command.

--attributeschema, -a

Name of attribute schema

--password-file, -f

File name that contains password of administrator.

--range, -r

End range

--schematype, -t

Type of schema.

--servicename, -s

Name of service.

[--subschemaname, -c]

Name of sub schema.

ssoadm set-attr-i18n-key

Set i18nKey member of attribute schema.

Usage: `ssoadm set-attr-i18n-key --options [--global-options]`

Options

--adminid, -u

Administrator ID of running the command.

--attributeschema, -a

Name of attribute schema

--i18nkey, -k

Attribute Schema I18n Key

--password-file, -f

File name that contains password of administrator.

--schematype, -t

Type of schema.

--servicename, -s

Name of service.

[--subschemaname, -c]

Name of sub schema.

ssoadm set-attr-start-range

Set attribute schema start range.

Usage: `ssoadm set-attr-start-range --options [--global-options]`

Options

`--adminid, -u`

Administrator ID of running the command.

`--attributeschema, -a`

Name of attribute schema

`--password-file, -f`

File name that contains password of administrator.

`--range, -r`

Start range

`--schematype, -t`

Type of schema.

`--servicename, -s`

Name of service.

`[--subschemaname, -c]`

Name of sub schema.

ssoadm set-attr-syntax

Set syntax member of attribute schema.

Usage: `ssoadm set-attr-syntax --options [--global-options]`

Options

`--adminid, -u`

Administrator ID of running the command.

`--attributeschema, -a`

Name of attribute schema

`--password-file, -f`

File name that contains password of administrator.

--schematype, -t

Type of schema.

--servicename, -s

Name of service.

--syntax, -x

Attribute Schema Syntax

[--subschemaname, -c]

Name of sub schema.

ssoadm set-attr-type

Set type member of attribute schema.

Usage: `ssoadm set-attr-type --options [--global-options]`

Options

--adminid, -u

Administrator ID of running the command.

--attributeschema, -a

Name of attribute schema

--password-file, -f

File name that contains password of administrator.

--schematype, -t

Type of schema.

--servicename, -s

Name of service.

--type, -p

Attribute Schema Type

[--subschemaname, -c]

Name of sub schema.

ssoadm set-attr-ui-type

Set UI type member of attribute schema.

Usage: `ssoadm set-attr-ui-type --options [--global-options]`

Options

`--adminid, -u`

Administrator ID of running the command.

`--attributeschema, -a`

Name of attribute schema

`--password-file, -f`

File name that contains password of administrator.

`--schematype, -t`

Type of schema.

`--servicename, -s`

Name of service.

`--uitype, -p`

Attribute Schema UI Type

`[--subschemaname, -c]`

Name of sub schema.

ssoadm set-attr-validator

Set attribute schema validator.

Usage: `ssoadm set-attr-validator --options [--global-options]`

Options

`--adminid, -u`

Administrator ID of running the command.

`--attributeschema, -a`

Name of attribute schema

--password-file, -f

File name that contains password of administrator.

--schematype, -t

Type of schema.

--servicename, -s

Name of service.

--validator, -r

validator class name

[--subschemaname, -c]

Name of sub schema.

ssoadm set-attr-view-bean-url

Set properties view bean URL member of attribute schema.

Usage: `ssoadm set-attr-view-bean-url --options [--global-options]`

Options

--adminid, -u

Administrator ID of running the command.

--attributeschema, -a

Name of attribute schema

--password-file, -f

File name that contains password of administrator.

--schematype, -t

Type of schema.

--servicename, -s

Name of service.

--url, -r

Attribute Schema Properties View Bean URL

[--subschemaname, -c]

Name of sub schema.

ssoadm set-entitlement-conf

Set entitlements service configuration

Usage: `ssoadm set-entitlement-conf --options [--global-options]`

Options

--adminid, -u

Administrator ID of running the command.

--password-file, -f

File name that contains password of administrator.

[--attributevalues, -a]

Attribute values e.g. evalThreadSize=4.

[--datafile, -D]

Name of file that contains attribute values data. Possible attributes are evalThreadSize, searchThreadSize, policyCacheSize and indexCacheSize.

ssoadm set-identity-attrs

Set attribute values of an identity

Usage: `ssoadm set-identity-attrs --options [--global-options]`

Options

--adminid, -u

Administrator ID of running the command.

--idname, -i

Name of identity.

--idtype, -t

Type of Identity such as User, Role and Group.

--password-file, -f

File name that contains password of administrator.

--realm, -e

Name of realm.

[--attributevalues, -a]

Attribute values e.g. homeaddress=here.

[--datafile, -D]

Name of file that contains attribute values data.

ssoadm set-identity-svc-attrs

Set service attribute values of an identity

Usage: `ssoadm set-identity-svc-attrs --options [--global-options]`

Options

--adminid, -u

Administrator ID of running the command.

--idname, -i

Name of identity.

--idtype, -t

Type of Identity such as User, Role and Group.

--password-file, -f

File name that contains password of administrator.

--realm, -e

Name of realm.

--servicename, -s

Name of service.

[--attributevalues, -a]

Attribute values e.g. homeaddress=here.

[--datafile, -D]

Name of file that contains attribute values data.

ssoadm set-inheritance

Set Inheritance value of Sub Schema.

Usage: `ssoadm set-inheritance --options [--global-options]`

Options

--adminid, -u

Administrator ID of running the command.

--inheritance, -r

Value of Inheritance.

--password-file, -f

File name that contains password of administrator.

--schematype, -t

Type of schema.

--servicename, -s

Name of service.

--subschemaname, -c

Name of sub schema.

ssoadm set-plugin-viewbean-url

Set properties view bean URL of plug-in schema.

Usage: `ssoadm set-plugin-viewbean-url --options [--global-options]`

Options

--adminid, -u

Administrator ID of running the command.

--interfacename, -i

Name of interface.

--password-file, -f

File name that contains password of administrator.

--pluginname, -g

Name of Plug-in.

--servicename, -s

Name of service.

--url, -r

Properties view bean URL.

ssoadm set-realm-attrs

Set attribute values of a realm.

Usage: `ssoadm set-realm-attrs --options [--global-options]`

Options

--adminid, -u

Administrator ID of running the command.

--password-file, -f

File name that contains password of administrator.

--realm, -e

Name of realm.

--servicename, -s

Name of service.

[--append, -p]

Set this flag to append the values to existing ones.

[--attributevalues, -a]

Attribute values e.g. homeaddress=here.

[--datafile, -D]

Name of file that contains attribute values data.

ssoadm set-realm-svc-attrs

Set attribute values of a service that is assigned to a realm. Long content for an attribute can be supplied in a file by appending '-file' to the attribute name, and giving the filename as the value.

Usage: `ssoadm set-realm-svc-attrs --options [--global-options]`

Options

--adminid, -u

Administrator ID of running the command.

--password-file, -f

File name that contains password of administrator.

--realm, -e

Name of realm.

--servicename, -s

Name of service.

[--append, -p]

Set this flag to append the values to existing ones.

[--attributevalues, -a]

Attribute values e.g. homeaddress=here.

[--datafile, -D]

Name of file that contains attribute values data.

ssoadm set-revision-number

Set service schema revision number.

Usage: `ssoadm set-revision-number --options [--global-options]`

Options

`--adminid, -u`

Administrator ID of running the command.

`--password-file, -f`

File name that contains password of administrator.

`--revisionnumber, -r`

Revision Number

`--servicename, -s`

Name of service.

ssoadm set-site-id

Set the ID of a site.

Usage: `ssoadm set-site-id --options [--global-options]`

Options

`--adminid, -u`

Administrator ID of running the command.

`--password-file, -f`

File name that contains password of administrator.

`--siteid, -i`

Site's ID, e.g. 10

`--sitename, -s`

Site name, e.g. mysite

ssoadm set-site-pri-url

Set the primary URL of a site.

Usage: `ssoadm set-site-pri-url --options [--global-options]`

Options

`--adminid, -u`

Administrator ID of running the command.

`--password-file, -f`

File name that contains password of administrator.

`--sitename, -s`

Site name, e.g. mysite

`--siteurl, -i`

Site's primary URL, e.g. http://site.www.example.com:8080

ssoadm set-site-sec-urls

Set Site Secondary URLs.

Usage: `ssoadm set-site-sec-urls --options [--global-options]`

Options

`--adminid, -u`

Administrator ID of running the command.

`--password-file, -f`

File name that contains password of administrator.

`--secondaryurls, -a`

Secondary URLs

`--sitename, -s`

Site name, e.g. mysite

ssoadm set-sub-cfg

Set sub configuration. Long content for an attribute can be supplied in a file by appending '-file' to the attribute name, and giving the filename as the value.

Usage: `ssoadm set-sub-cfg --options [--global-options]`

Options

`--adminid, -u`

Administrator ID of running the command.

`--operation, -o`

Operation (either add/set/delete) to be performed on the sub configuration.

`--password-file, -f`

File name that contains password of administrator.

`--servicename, -s`

Name of service.

`--subconfigname, -g`

Name of sub configuration.

`[--attributevalues, -a]`

Attribute values e.g. homeaddress=here.

`[--datafile, -D]`

Name of file that contains attribute values data.

`[--realm, -e]`

Name of realm (Sub Configuration shall be set to global configuration if this option is not provided).

ssoadm set-svc-attrs

Set service attribute values in a realm. Long content for an attribute can be supplied in a file by appending '-file' to the attribute name, and giving the filename as the value.

Usage: `ssoadm set-svc-attrs --options [--global-options]`

Options

`--adminid, -u`

Administrator ID of running the command.

--password-file, -f

File name that contains password of administrator.

--realm, -e

Name of realm.

--servicename, -s

Name of service.

[--attributevalues, -a]

Attribute values e.g. homeaddress=here.

[--datafile, -D]

Name of file that contains attribute values data.

ssoadm set-svc-i18n-key

Set service schema i18n key.

Usage: `ssoadm set-svc-i18n-key --options [--global-options]`

Options

--adminid, -u

Administrator ID of running the command.

--i18nkey, -k

I18n Key.

--password-file, -f

File name that contains password of administrator.

--servicename, -s

Name of service.

ssoadm set-svc-view-bean-url

Set service schema properties view bean URL.

Usage: `ssoadm set-svc-view-bean-url --options [--global-options]`

Options

`--adminid, -u`

Administrator ID of running the command.

`--password-file, -f`

File name that contains password of administrator.

`--servicename, -s`

Name of service.

`--url, -r`

Service Schema Properties View Bean URL

ssoadm set-svrcfg-xml

Set server configuration XML to centralized data store

Usage: `ssoadm set-svrcfg-xml --options [--global-options]`

Options

`--adminid, -u`

Administrator ID of running the command.

`--password-file, -f`

File name that contains password of administrator.

`--servername, -s`

Server name, e.g. http://www.example.com:8080/fam

`--xmlfile, -X`

XML file that contains configuration.

ssoadm show-agent

Show agent profile.

Usage: `ssoadm show-agent --options [--global-options]`

Options

`--adminid, -u`

Administrator ID of running the command.

`--agentname, -b`

Name of agent.

`--password-file, -f`

File name that contains password of administrator.

`--realm, -e`

Name of realm.

`[--includepassword, -p]`

Include the hashed password in the export.

`[--inherit, -i]`

Set this to inherit properties from parent group.

`[--outfile, -o]`

Filename where configuration is written to.

ssoadm show-agent-grp

Show agent group profile.

Usage: `ssoadm show-agent-grp --options [--global-options]`

Options

`--adminid, -u`

Administrator ID of running the command.

`--agentgroupname, -b`

Name of agent group.

`--password-file, -f`

File name that contains password of administrator.

--realm, -e

Name of realm.

[--outfile, -o]

Filename where configuration is written to.

ssoadm show-agent-membership

List agent's membership.

Usage: `ssoadm show-agent-membership --options [--global-options]`

Options

--adminid, -u

Administrator ID of running the command.

--agentname, -b

Name of agent.

--password-file, -f

File name that contains password of administrator.

--realm, -e

Name of realm.

ssoadm show-agent-types

Show agent types.

Usage: `ssoadm show-agent-types --options [--global-options]`

Options

--adminid, -u

Administrator ID of running the command.

--password-file, -f

File name that contains password of administrator.

ssoadm show-app-priv

Show policy set privilege.

Usage: `ssoadm show-app-priv --options [--global-options]`

Options

`--adminid, -u`

Administrator ID of running the command.

`--name, -m`

Name of policy set privilege

`--password-file, -f`

File name that contains password of administrator.

`--realm, -e`

Realm name

ssoadm show-appl

Show policy set attributes.

Usage: `ssoadm show-appl --options [--global-options]`

Options

`--adminid, -u`

Administrator ID of running the command.

`--name, -m`

Policy set name

`--password-file, -f`

File name that contains password of administrator.

`--realm, -e`

Realm name

ssoadm show-appl-type

Show application type details.

Usage: `ssoadm show-appl-type --options [--global-options]`

Options

`--adminid, -u`

Administrator ID of running the command.

`--name, -m`

Application Type name

`--password-file, -f`

File name that contains password of administrator.

ssoadm show-auth-modules

Show the supported authentication modules in the system.

Usage: `ssoadm show-auth-modules --options [--global-options]`

Options

`--adminid, -u`

Administrator ID of running the command.

`--password-file, -f`

File name that contains password of administrator.

ssoadm show-data-types

Show the supported data type in the system.

Usage: `ssoadm show-data-types --options [--global-options]`

Options

`--adminid, -u`

Administrator ID of running the command.

--password-file, -f

File name that contains password of administrator.

ssoadm show-datastore

Show data store profile.

Usage: `ssoadm show-datastore --options [--global-options]`

Options

--adminid, -u

Administrator ID of running the command.

--name, -m

Name of datastore.

--password-file, -f

File name that contains password of administrator.

--realm, -e

Name of realm.

ssoadm show-entitlement-conf

Display entitlements service configuration

Usage: `ssoadm show-entitlement-conf --options [--global-options]`

Options

--adminid, -u

Administrator ID of running the command.

--password-file, -f

File name that contains password of administrator.

ssoadm show-identity-ops

Show the allowed operations of an identity a realm

Usage: `ssoadm show-identity-ops --options [--global-options]`

Options

`--adminid, -u`

Administrator ID of running the command.

`--idtype, -t`

Type of Identity such as User, Role and Group.

`--password-file, -f`

File name that contains password of administrator.

`--realm, -e`

Name of realm.

ssoadm show-identity-svc-attrs

Show the service attribute values of an identity

Usage: `ssoadm show-identity-svc-attrs --options [--global-options]`

Options

`--adminid, -u`

Administrator ID of running the command.

`--idname, -i`

Name of identity.

`--idtype, -t`

Type of Identity such as User, Role and Group.

`--password-file, -f`

File name that contains password of administrator.

`--realm, -e`

Name of realm.

`--servicename, -s`

Name of service.

ssoadm show-identity-types

Show the supported identity type in a realm

Usage: `ssoadm show-identity-types --options [--global-options]`

Options

`--adminid, -u`

Administrator ID of running the command.

`--password-file, -f`

File name that contains password of administrator.

`--realm, -e`

Name of realm.

ssoadm show-members

Show the members of an identity. For example show the members of a role

Usage: `ssoadm show-members --options [--global-options]`

Options

`--adminid, -u`

Administrator ID of running the command.

`--idname, -i`

Name of identity.

`--idtype, -t`

Type of Identity such as User, Role and Group.

`--membershipidtype, -m`

Membership identity type.

`--password-file, -f`

File name that contains password of administrator.

`--realm, -e`

Name of realm.

ssoadm show-memberships

Show the memberships of an identity. For sample show the memberships of an user.

Usage: `ssoadm show-memberships --options [--global-options]`

Options

`--adminid, -u`

Administrator ID of running the command.

`--idname, -i`

Name of identity.

`--idtype, -t`

Type of Identity such as User, Role and Group.

`--membershipidtype, -m`

Membership identity type.

`--password-file, -f`

File name that contains password of administrator.

`--realm, -e`

Name of realm.

ssoadm show-privileges

Show privileges assigned to an identity

Usage: `ssoadm show-privileges --options [--global-options]`

Options

`--adminid, -u`

Administrator ID of running the command.

`--idname, -i`

Name of identity.

--idtype, -t

Type of Identity such Role and Group.

--password-file, -f

File name that contains password of administrator.

--realm, -e

Name of realm.

ssoadm show-realm-svcs

Show services in a realm.

Usage: `ssoadm show-realm-svcs --options [--global-options]`

Options

--adminid, -u

Administrator ID of running the command.

--password-file, -f

File name that contains password of administrator.

--realm, -e

Name of realm.

[--mandatory, -y]

Include Mandatory services.

ssoadm show-site

Show site profile.

Usage: `ssoadm show-site --options [--global-options]`

Options

--adminid, -u

Administrator ID of running the command.

--password-file, -f

File name that contains password of administrator.

--sitename, -s

Site name, e.g. mysite

ssoadm show-site-members

Display members of a site.

Usage: `ssoadm show-site-members --options [--global-options]`

Options

--adminid, -u

Administrator ID of running the command.

--password-file, -f

File name that contains password of administrator.

--sitename, -s

Site name, e.g. mysite

ssoadm start-recording

Start recording a bundle that contains troubleshooting information, including debug logs, thread dumps, and environment information.

Usage: `ssoadm start-recording --options [--global-options]`

Options

--adminid, -u

Administrator ID of running the command.

--jsonfile, -J

JSON control file for a recording operation.

--password-file, -f

File name that contains password of administrator.

--servername, -s

Server name, e.g. http://openam.example.com:8080/openam

ssoadm stop-recording

Stop an active recording operation.

Usage: `ssoadm stop-recording --options [--global-options]`

Options

--adminid, -u

Administrator ID of running the command.

--password-file, -f

File name that contains password of administrator.

--servername, -s

Server name, e.g. http://openam.example.com:8080/openam

ssoadm unregister-auth-module

Unregisters authentication module.

Usage: `ssoadm unregister-auth-module --options [--global-options]`

Options

--adminid, -u

Administrator ID of running the command.

--authmodule, -a

Java class name of authentication module.

--password-file, -f

File name that contains password of administrator.

ssoadm update-agent

Update agent configuration.

Usage: `ssoadm update-agent --options [--global-options]`

Options

`--adminid, -u`

Administrator ID of running the command.

`--agentname, -b`

Name of agent.

`--password-file, -f`

File name that contains password of administrator.

`--realm, -e`

Name of realm.

`[--attributevalues, -a]`

Properties e.g. homeaddress=here.

`[--datafile, -D]`

Name of file that contains properties.

`[--set, -s]`

Set this flag to overwrite properties values.

ssoadm update-agent-grp

Update agent group configuration.

Usage: `ssoadm update-agent-grp --options [--global-options]`

Options

`--adminid, -u`

Administrator ID of running the command.

`--agentgroupname, -b`

Name of agent group.

--password-file, -f

File name that contains password of administrator.

--realm, -e

Name of realm.

[--attributevalues, -a]

Properties e.g. homeaddress=here.

[--datafile, -D]

Name of file that contains properties.

[--set, -s]

Set this flag to overwrite properties values.

ssoadm update-app-priv

Update a policy set privilege.

Usage: `ssoadm update-app-priv --options [--global-options]`

Options

--adminid, -u

Administrator ID of running the command.

--name, -m

Name for the this delegation

--password-file, -f

File name that contains password of administrator.

--realm, -e

Realm name

[--actions, -a]

Possible values are READ, MODIFY, DELEGATE, ALL

[--description, -p]

Description for the this delegation.

ssoadm update-app-priv-resources

Set policy set privilege resources. Note that policy sets are cached for 30 minutes. Restart OpenAM to apply changes immediately.

Usage: `ssoadm update-app-priv-resources --options [--global-options]`

Options

`--adminid, -u`

Administrator ID of running the command.

`--application, -t`

Policy set name

`--name, -m`

Name for the this delegation

`--password-file, -f`

File name that contains password of administrator.

`--realm, -e`

Realm name

`[--add, -p]`

Resources are added to this policy set if this option is set. Otherwise, resources in the current policy set privilege will be overwritten.

`[--resources, -r]`

Resources to delegate, All resources in the policy set will be delegated if this option is absent.

ssoadm update-app-priv-subjects

Set policy set privilege subjects.

Usage: `ssoadm update-app-priv-subjects --options [--global-options]`

Options

`--adminid, -u`

Administrator ID of running the command.

--name, -m

Name for the this delegation

--password-file, -f

File name that contains password of administrator.

--realm, -e

Realm name

--subjects, -s

Subject name

--subjecttype, -b

Possible values are User or Group

[--add, -p]

Subjects are added to this policy set if this option is set. Otherwise, subjects in the current policy set privilege will be overwritten.

ssoadm update-auth-cfg-entr

Set authentication configuration entries

Usage: `ssoadm update-auth-cfg-entr --options [--global-options]`

Options

--adminid, -u

Administrator ID of running the command.

--name, -m

Name of authentication configuration.

--password-file, -f

File name that contains password of administrator.

--realm, -e

Name of realm.

[--datafile, -D]

Name of file that contains formatted authentication configuration entries in this format name|flag|options. option can be REQUIRED, OPTIONAL, SUFFICIENT, REQUISITE. e.g. myauthmodule|REQUIRED|my options.

[--entries, -a]

formatted authentication configuration entries in this format name|flag|options. option can be REQUIRED, OPTIONAL, SUFFICIENT, REQUISITE. e.g. myauthmodule|REQUIRED|my options.

ssoadm update-auth-cfg-props

Set authentication configuration properties

Usage: `ssoadm update-auth-cfg-props --options [--global-options]`

Options

--adminid, -u

Administrator ID of running the command.

--name, -m

Name of authentication configuration.

--password-file, -f

File name that contains password of administrator.

--realm, -e

Name of realm.

[--attributevalues, -a]

authentication configuration properties, valid configuration keys are: iplanet-am-auth-login-failure-url, iplanet-am-auth-login-success-url and iplanet-am-auth-post-login-process-class.

[--datafile, -D]

Name of file that contains authentication configuration properties.

ssoadm update-auth-instance

Update authentication instance values

Usage: `ssoadm update-auth-instance --options [--global-options]`

Options

`--adminid, -u`

Administrator ID of running the command.

`--name, -m`

Name of authentication instance.

`--password-file, -f`

File name that contains password of administrator.

`--realm, -e`

Name of realm.

`[--attributevalues, -a]`

Attribute values e.g. homeaddress=here.

`[--datafile, -D]`

Name of file that contains attribute values data.

ssoadm update-datastore

Update data store profile.

Usage: `ssoadm update-datastore --options [--global-options]`

Options

`--adminid, -u`

Administrator ID of running the command.

`--name, -m`

Name of datastore.

`--password-file, -f`

File name that contains password of administrator.

`--realm, -e`

Name of realm.

[--attributevalues, -a]

Attribute values e.g. sunIdRepoClass=com.sun.identity.idm.plugins.files.FilesRepo.

[--datafile, -D]

Name of file that contains attribute values data.

ssoadm update-entity-keyinfo

Update XML signing and encryption key information in hosted entity metadata.

Usage: `ssoadm update-entity-keyinfo --options [--global-options]`

Options

--adminid, -u

Administrator ID of running the command.

--entityid, -y

Entity ID

--password-file, -f

File name that contains password of administrator.

[--idpecertalias, -g]

Identity provider encryption certificate aliases.

[--idpscertalias, -b]

Identity provider signing certificate aliases

[--realm, -e]

Realm where entity resides.

[--specertalias, -r]

Service provider encryption certificate aliases

[--spec, -c]

Specify metadata specification, either wsfed, idff or saml2, defaults to saml2

[--spscertalias, -a]

Service provider signing certificate aliases

ssoadm update-server-cfg

Update server configuration.

Usage: `ssoadm update-server-cfg --options [--global-options]`

Options

`--adminid, -u`

Administrator ID of running the command.

`--password-file, -f`

File name that contains password of administrator.

`--servername, -s`

Server name, e.g. http://www.example.com:8080/fam or enter default to update default server configuration.

`[--attributevalues, -a]`

Attribute values e.g. homeaddress=here.

`[--datafile, -D]`

Name of file that contains attribute values data.

ssoadm update-svc

Update service.

Usage: `ssoadm update-svc --options [--global-options]`

Options

`--adminid, -u`

Administrator ID of running the command.

`--password-file, -f`

File name that contains password of administrator.

`--xmlfile, -X`

XML file(s) that contains schema.

[--continue, -c]

Continue updating service if one or more previous services cannot be updated.

Using Multiple Attributes in a Single ssoadm Command

You can set multiple attributes in a single **ssoadm** command by using a text file or by specifying multiple attributes with the **-a** option.

Text File

1. Create a text file with each property on each line followed by a line feed and save the file for example, as `TEXT_FILE`:

```
iplanet-am-session-max-session-time=150
iplanet-am-session-max-idle-time=15
iplanet-am-session-max-caching-time=5
```

2. Run the **ssoadm** command specifying the name of the file with the **--datafile** (`-D`) option:

```
$ ./ssoadm set-attr-defs \
  --servicename iPlanetAMSessionService \
  --schematype dynamic \
  --adminid uid=amAdmin,ou=People,dc=openam,dc=forgerock,dc=org \
  --password-file passwordfile \
  --datafile TEXT_FILE
```

Using the **--attributevalues** Option

Run **ssoadm** using the **--attributevalues** (`-a`) option. Separate each attribute with a space.

```
$ ./ssoadm set-attr-defs \
  --servicename iPlanetAMSessionService \
  --schematype dynamic \
  --adminid uid=amAdmin,ou=People,dc=openam,dc=forgerock,dc=org \
  --password-file passwordfile \
  --attributevalues \
      iplanet-am-session-max-session-time=150 \
      iplanet-am-session-max-idle-time=15 \
      iplanet-am-session-max-caching-time=5
```

Chapter 2

Authentication Configuration

As described in the "*Configuring AM for Authentication*" in the *Authentication and Single Sign-On Guide*, you configure authentication by realm at the following locations in the AM console:

- Under Realms > *Realm Name* > Authentication > Settings
- Under Realms > *Realm Name* > Authentication > Modules

You can configure default values for authentication modules under Configure > Authentication using the same attributes you use to configure authentication modules per realm. These defaults are used when a module is created for a specific realm.

The core attributes page includes some fields that are not available under Realms > *Realm Name* > Authentication > Settings. Because attributes set under Configure > Authentication > Core Attributes apply on a server level, the changes you make here will apply to all realms. Attributes set by Realm only apply to the realm that you specify. The Authentication Module Defaults list under Configure > Authentication shows all existing types of modules available for configuration, including any customized modules you have added.

The following section describes the properties you can configure on the Global tab under Configure > Authentication > Core Attributes. The properties on the other tabs on that page are described in "Core Authentication Attributes" in the *Authentication and Single Sign-On Guide*.

\+ *Global Attributes*

The following properties are available under the Global Attributes tab:

Pluggable Authentication Module Classes

Lists the authentication modules classes available to AM. If you have custom authentication modules, add classes to this list that extend from the `com.sun.identity.authentication.spi.AMLoginModule` class.

For more information about custom authentication modules, see "Creating a Custom Authentication Module" in the *Authentication and Single Sign-On Guide*.

amster attribute: `authenticators`

ssoadm attribute: `iplanet-am-auth-authenticators`

LDAP Connection Pool Size

Sets a minimum and a maximum number of LDAP connections to be used by any authentication module that connects to a specific directory server. This connection pool is different than the SDK connection pool configured in `serverconfig.xml` file.

Format is `host:port:minimum:maximum`.

This attribute is for LDAP and Membership authentication modules only.

amster attribute: `ldapConnectionPoolSize`

ssoadm attribute: `iplanet-am-auth-ldap-connection-pool-size`

Default LDAP Connection Pool Size

Sets the default minimum and maximum number of LDAP connections to be used by any authentication module that connects to any directory server. This connection pool is different than the SDK connection pool configured in `serverconfig.xml` file.

Format is `minimum:maximum`.

When tuning for production, start with 10 minimum, 65 maximum. For example, `10:65`.

This attribute is for LDAP and Membership authentication modules only.

amster attribute: `ldapConnectionPoolDefaultSize`

ssoadm attribute: `iplanet-am-auth-ldap-connection-pool-default-size`

Remote Auth Security

When enabled, AM requires the authenticating application to send its SSO token. This allows AM to obtain the username and password associated with the application.

amster attribute: `remoteAuthSecurityEnabled`

ssoadm attribute: `sunRemoteAuthSecurityEnabled`

Keep Post Process Objects for Logout Processing

When enabled, AM stores instances of post-processing classes into the user session. When the user logs out, the original post-processing classes are called instead of new instances. This may be required for special logout processing.

Enabling this setting increases the memory usage of AM.

amster attribute: `keepPostProcessInstances`

ssoadm attribute: `sunAMAuthKeepPostProcessInstances`

+ *Core*

The following properties are available under the Core tab:

Administrator Authentication Configuration

Specifies the default authentication chain used when an administrative user, such as `amAdmin`, logs in to the AM console.

ssoadm attribute:`iplanet-am-auth-admin-auth-module`

Organization Authentication Configuration

Specifies the default authentication chain used when a non-administrative user logs in to AM.

amster attribute: `orgConfig`

ssoadm attribute: `iplanet-am-auth-org-config`

+ *User Profile*

The following properties are available under the User Profile tab:

`User Profile`

Specifies whether a user profile needs to exist in the user data store, or should be created on successful authentication. The possible values are:

`true`**. Dynamic.**

After successful authentication, AM creates a user profile if one does not already exist. AM then issues the SSO token. AM creates the user profile in the user data store configured for the realm.

`createAlias`**. Dynamic with User Alias.**

After successful authentication, AM creates a user profile that contains the `User Alias List` attribute, which defines one or more aliases for mapping a user's multiple profiles.

`ignore`**. Ignored.**

After successful authentication, AM issues an SSO token regardless of whether a user profile exists in the data store. The presence of a user profile is not checked.

Warning

Any functionality which needs to map values to profile attributes, such as SAML or OAuth 2.0, will not operate correctly if the User Profile property is set to `ignore`.

`false`. **Required.**

After successful authentication, the user must have a user profile in the user data store configured for the realm in order for AM to issue an SSO token.

ssoadm attribute: `iplanet-am-auth-dynamic-profile-creation`. Set this attribute's value to one of the following: `true`, `createAlias`, `ignore`, or `false`.

User Profile Dynamic Creation Default Roles

Specifies the distinguished name (DN) of a role to be assigned to a new user whose profile is created when either the `true` or `createAlias` options are selected under the User Profile property. There are no default values. The role specified must be within the realm for which the authentication process is configured.

This role can be either an AM or Sun DSEE role, but it cannot be a filtered role. If you wish to automatically assign specific services to the user, you have to configure the Required Services property in the user profile.

This functionality is *deprecated*.

amster attribute: `defaultRole`

ssoadm attribute: `iplanet-am-auth-default-role`

Alias Search Attribute Name

After a user is successfully authenticated, the user's profile is retrieved. AM first searches for the user based on the data store settings. If that fails to find the user, AM will use the attributes listed here to look up the user profile. This setting accepts any data store specific attribute name.

amster attribute: `aliasAttributeName`

ssoadm attribute: `iplanet-am-auth-alias-attr-name`

Note

If the `Alias Search Attribute Name` property is empty, AM uses the `iplanet-am-auth-user-naming-attr` property from the `iPlanetAmAuthService`. The `iplanet-am-auth-user-naming-attr` property is only configurable through the **ssoadm** command-line tool and not through the AM console.

```
$ ssoadm get-realm-svc-attrs \
--adminid uid=amAdmin,ou=People,dc=openam,dc=forgerock,dc=org \
--password-file PATH_TO_PWDFILE \
--realm REALM \
--servicename iPlanetAMAuthService

$ ssoadm set-realm-svc-attrs \
 --adminid uid=amAdmin,ou=People,dc=openam,dc=forgerock,dc=org \
 --password-file PATH_TO_PWDFILE \
 --realm REALM \
 --servicename iPlanetAMAuthService \
 --attributevalues iplanet-am-auth-user-naming-attr=SEARCH_ATTRIBUTE
```

+ *Account Lockout*

The following properties are available under the Account Lockout tab:

Login Failure Lockout Mode

When enabled, AM deactivates the LDAP attribute defined in the Lockout Attribute Name property in the user's profile upon login failure. This attribute works in conjunction with the other account lockout and notification attributes.

amster attribute: `loginFailureLockoutMode`

ssoadm attribute: `iplanet-am-auth-login-failure-lockout-mode`

Login Failure Lockout Count

Defines the number of attempts that a user has to authenticate within the time interval defined in Login Failure Lockout Interval before being locked out.

amster attribute: `loginFailureCount`

ssoadm attribute: `iplanet-am-auth-login-failure-count`

Login Failure Lockout Interval

Defines the time in minutes during which failed login attempts are counted. If one failed login attempt is followed by a second failed attempt within this defined lockout interval time, the lockout count starts, and the user is locked out if the number of attempts reaches the number defined by the Login Failure Lockout Count property. If an attempt within the defined lockout interval time proves successful before the number of attempts reaches the number defined by the Login Failure Lockout Count property, the lockout count is reset.

amster attribute: `loginFailureDuration`

ssoadm attribute: `iplanet-am-auth-login-failure-duration`

Email Address to Send Lockout Notification

Specifies one or more email addresses to which notification is sent if a user lockout occurs.

Separate multiple addresses with spaces, and append `|locale|charset` to addresses for recipients in non-English locales.

amster attribute: `lockoutEmailAddress`

ssoadm attribute: `iplanet-am-auth-lockout-email-address`

Warn User After N Failures

Specifies the number of authentication failures after which AM displays a warning message that the user will be locked out.

ssoadm attribute: `iplanet-am-auth-lockout-warn-user`

Login Failure Lockout Duration

Defines how many minutes a user must wait after a lockout before attempting to authenticate again. Entering a value greater than 0 enables memory lockout and disables physical lockout. *Memory lockout* means the user's account is locked in memory for the number of minutes specified. The account is unlocked after the time period has passed.

amster attribute: `lockoutDuration`

ssoadm attribute: `iplanet-am-auth-lockout-duration`

Lockout Duration Multiplier

Defines a value with which to multiply the value of the Login Failure Lockout Duration attribute for each successive lockout. For example, if Login Failure Lockout Duration is set to 3 minutes, and the Lockout Duration Multiplier is set to 2, the user is locked out of the account for 6 minutes. After the 6 minutes has elapsed, if the user again provides the wrong credentials, the lockout duration is then 12 minutes. With the Lockout Duration Multiplier, the lockout duration is incrementally increased based on the number of times the user has been locked out.

amster attribute: `lockoutDurationMultiplier`

ssoadm attribute: `sunLockoutDurationMultiplier`

Lockout Attribute Name

Defines the LDAP attribute used for physical lockout. The default attribute is `inetuserstatus`, although the field in the AM console is empty. The Lockout Attribute Value field must also contain an appropriate value.

amster attribute: `lockoutAttributeName`

ssoadm attribute: `iplanet-am-auth-lockout-attribute-name`

Lockout Attribute Value

Specifies the action to take on the attribute defined in Lockout Attribute Name. The default value is `inactive`, although the field in the AM console is empty. The Lockout Attribute Name field must also contain an appropriate value.

amster attribute: `lockoutAttributeValue`

ssoadm attribute: `iplanet-am-auth-lockout-attribute-value`

Invalid Attempts Data Attribute Name

Specifies the LDAP attribute used to hold the number of failed authentication attempts towards Login Failure Lockout Count. Although the field appears empty in the AM console, AM stores this data in the `sunAMAuthInvalidAttemptsDataAttrName` attribute defined in the `sunAMAuthAccountLockout` objectclass by default.

amster attribute: `invalidAttemptsDataAttributeName`

ssoadm attribute: `sunAMAuthInvalidAttemptsDataAttrName`

Store Invalid Attempts in Data Store

When enabled, AM stores the information regarding failed authentication attempts as the value of the Invalid Attempts Data Attribute Name in the user data store. Information stored includes number of invalid attempts, time of last failed attempt, lockout time and lockout duration. Storing this information in the identity repository allows it to be shared among multiple instances of AM.

Enable this property to track invalid log in attempts when using CTS-based or client-based authentication sessions.

amster attribute: `storeInvalidAttemptsInDataStore`

ssoadm attribute: `sunStoreInvalidAttemptsInDS`

+ *General*

The following properties are available under the General tab:

Default Authentication Locale

Specifies the default language subtype to be used by the Authentication Service. The default value is `en_US`.

amster attribute: `locale`

ssoadm attribute: `iplanet-am-auth-locale`

Identity Types

Lists the type or types of identities used during a profile lookup. You can choose more than one to search on multiple types if you would like AM to conduct a second lookup if the first lookup fails. The possible values are:

`Agent`

Searches for identities under your agents.

`agentgroup`

Searches for identities according to your established agent group.

`agentonly`

Searches for identities only under your agents.

`Group`

Searches for identities according to your established groups.

`User`

Searches for identities according to your users.

Default: `Agent` and `User`.

amster attribute: `identityType`

ssoadm attribute: `sunAMIdentityType`

Pluggable User Status Event Classes

Specifies one or more Java classes used to provide a callback mechanism for user status changes during the authentication process. The Java class must implement the `com.sun.identity.authentication.spi.AMAuthCallBack` interface. AM supports account lockout and password changes. AM supports password changes through the LDAP authentication module, and so the feature is only available for the LDAP module.

A `.jar` file containing the user status event class belongs in the `WEB-INF/lib` directory of the deployed AM instance. If you do not build a `.jar` file, add the class files under `WEB-INF/classes`.

amster attribute: `userStatusCallbackPlugins`

ssoadm attribute: `sunAMUserStatusCallbackPlugins`

Use Client-Based Sessions

When enabled, AM assigns *client-based* sessions to users authenticating to this realm. Otherwise, AM users authenticating to this realm are assigned *CTS-based* sessions.

For more information about sessions, see "*Introducing Sessions*" in the *Sessions Guide*.

amster attribute: `statelessSessionsEnabled`

ssoadm attribute: `openam-auth-stateless-sessions`

Two Factor Authentication Mandatory

When enabled, users authenticating to a chain that includes a ForgeRock Authenticator (OATH) module are always required to perform authentication using a registered device before they can access AM. When not selected, users can opt to forego registering a device and providing a token and still successfully authenticate.

Letting users choose not to provide a verification token while authenticating carries implications beyond the `required`, `optional`, `requisite`, or `sufficient` flag settings on the ForgeRock Authenticator (OATH) module in the authentication chain. For example, suppose you configured authentication as follows:

- The ForgeRock Authenticator (OATH) module is in an authentication chain.
- The ForgeRock Authenticator (OATH) module has the `required` flag set.
- Two Factor Authentication Mandatory is not selected.

Users authenticating to the chain can authenticate successfully *without* providing tokens from their devices. The reason for successful authentication in this case is that the `required` setting relates to the execution of the ForgeRock Authenticator (OATH) module itself. Internally, the ForgeRock Authenticator (OATH) module has the ability to forego processing a token while still returning a passing status to the authentication chain.

Note

The `Two Factor Authentication Mandatory` property only applies to modules within authentication chains, and does not affect nodes within authentication trees.

amster attribute: `twoFactorRequired`

ssoadm attribute: `forgerockTwoFactorAuthMandatory`

External Login Page URL

Specifies the URL of the external login user interface, if the authentication user interface is hosted separately from AM.

When set, AM will use the provided URL as the base of the resume URI, rather than using the Base URL Source Service to obtain the base URL. AM will use this URL when constructing the resume URI if authentication is suspended in an authentication tree.

For more information about the Base URL Source Service, see "Configuring the Base URL Source Service" in the *Security Guide*.

amster attribute: `externalLoginPageUrl`

ssoadm attribute: `externalLoginPageUrl`

Default Authentication Level

Specifies the default authentication level for authentication modules.

amster attribute: `defaultAuthLevel`

ssoadm attribute: `iplanet-am-auth-default-auth-level`

+ *Security*

The following properties are available under the Security tab:

Module Based Authentication

When enabled, users can authenticate using module-based authentication. Otherwise, all attempts at authentication using the `module=module-name` login parameter result in failure.

ForgeRock recommends disabling module-based authentication in production environments.

amster attribute: `moduleBasedAuthEnabled`

ssoadm attribute: `sunEnableModuleBasedAuth`

Persistent Cookie Encryption Certificate Alias

Specifies the key pair alias in the AM keystore to use for encrypting persistent cookies.

Default: `test`

amster attribute: `keyAlias`

ssoadm attribute: `iplanet-am-auth-key-alias`

Zero Page Login

When enabled, AM allows users to authenticate using only GET request parameters without showing a login screen.

Caution

Enable with caution as browsers can cache credentials and servers can log credentials when they are part of the URL.

AM always allows HTTP POST requests for zero page login.

Default: false (disabled)

amster attribute: `zeroPageLoginEnabled`

ssoadm attribute: `openam.auth.zero.page.login.enabled`

Zero Page Login Referer Whitelist

Lists the HTTP referer URLs for which AM allows zero page login. These URLs are supplied in the `Referer` HTTP request header, allowing clients to specify the web page that provided the link to the requested resource.

When zero page login is enabled, including the URLs for the pages from which to allow zero page login will provide some mitigation against Login Cross-Site Request Forgery (CSRF) attacks. Leave this list blank to allow zero page login from any Referer.

This setting applies for both HTTP GET and also HTTP POST requests for zero page login.

amster attribute: `zeroPageLoginReferrerWhiteList`

ssoadm attribute: `openam.auth.zero.page.login.referer.whitelist`

Zero Page Login Allowed Without Referer?

When enabled, allows zero page login for requests without an HTTP `Referer` request header. Zero page login must also be enabled.

Enabling this setting reduces the risk of login CSRF attacks with zero page login enabled, but may potentially deny legitimate requests.

amster attribute: `zeroPageLoginAllowedWithoutReferrer`

ssoadm attribute: `openam.auth.zero.page.login.allow.null.referer`

Organization Authentication Signing Secret

Specifies a cryptographically-secure random-generated HMAC shared secret for signing RESTful authentication requests. When users attempt to authenticate to the UI, AM signs a JSON Web Token (JWT) containing this shared secret. The JWT contains the authentication session ID, realm, and authentication index type value, but does *not* contain the user's credentials.

When modifying this value, ensure the new shared secret is Base-64 encoded and at least 128 bits in length.

amster attribute: `sharedSecret`

ssoadm attribute: `iplanet-am-auth-hmac-signing-shared-secret`

+ *Post Authentication Processing*

The following properties are available under the Post Authentication Processing tab:

Default Success Login URL

Accepts a list of values that specifies where users are directed after successful authentication. The format of this attribute is *client-type|URL* although the only value you can specify at this time is a URL which assumes the type HTML. The default value is `/openam/console`. Values that do not specify HTTP have that appended to the deployment URI.

amster attribute: `loginSuccessUrl`

ssoadm attribute: `iplanet-am-auth-login-success-url`

Default Failure Login URL

Accepts a list of values that specifies where users are directed after authentication has failed. The format of this attribute is *client-type|URL* although the only value you can specify at this time is a URL which assumes the type HTML. Values that do not specify HTTP have that appended to the deployment URI.

amster attribute: `loginFailureUrl`

ssoadm attribute: `iplanet-am-auth-login-failure-url`

Authentication Post Processing Classes

Specifies one or more Java classes used to customize post authentication processes for successful or unsuccessful logins. The Java class must implement the `com.sun.identity.authentication.spi.AMPostAuthProcessInterface` AM interface.

A `.jar` file containing the post processing class belongs in the `WEB-INF/lib` directory of the deployed AM instance. If you do not build a `.jar` file, add the class files under `WEB-INF/classes`. For deployment, add the `.jar` file or classes into a custom AM `.war` file.

For information on creating post-authentication plugins, see "Creating Post-Authentication Plugins for Chains" in the *Authentication and Single Sign-On Guide*.

amster attribute: `loginPostProcessClass`

ssoadm attribute: `iplanet-am-auth-post-login-process-class`

Generate UserID Mode

When enabled, the Membership module generates a list of alternate user identifiers if the one entered by a user during the self-registration process is not valid or already exists. The user IDs are generated by the class specified in the Pluggable User Name Generator Class property.

amster attribute: `usernameGeneratorEnabled`

ssoadm attribute: `iplanet-am-auth-username-generator-enabled`

Pluggable User Name Generator Class

Specifies the name of the class used to generate alternate user identifiers when Generate UserID Mode is enabled. The default value is `com.sun.identity.authentication.spi.DefaultUserIDGenerator`.

amster attribute: `usernameGeneratorClass`

ssoadm attribute: `iplanet-am-auth-username-generator-class`

User Attribute Mapping to Session Attribute

Enables the authenticating user's identity attributes (stored in the identity repository) to be set as session properties in the user's SSO token. The value takes the format *`User-Profile-Attribute|Session-Attribute-Name`*. If *Session-Attribute-Name* is not specified, the value of *User-Profile-Attribute* is used. All session attributes contain the `am.protected` prefix to ensure that they cannot be edited by the client applications.

For example, if you define the user profile attribute as `mail` and the user's email address, available in the user session, as `user.mail`, the entry for this attribute would be `mail|user.mail`. After a successful authentication, the `SSOToken.getProperty(String)` method is used to retrieve the user profile attribute set in the session. The user's email address is retrieved from the user's session using the `SSOToken.getProperty("am.protected.user.mail")` method call.

Properties that are set in the user session using User Attribute Mapping to Session Attributes cannot be modified (for example, `SSOToken.setProperty(String, String)`). This results in an `SSOException`. Multivalued attributes, such as `memberOf`, are listed as a single session variable with a `|` separator.

When configuring authentication for a realm configured for client-based sessions, be careful not to add so many session attributes that the session cookie size exceeds the maximum allowable cookie size. For more information about client-based session cookies, see "*Session Cookies and Session Security*" in the *Sessions Guide*.

amster attribute: `userAttributeSessionMapping`

ssoadm attribute: `sunAMUserAttributesSessionMapping`

Important

The `User Attribute Mapping to Session Attribute` property only applies to modules within authentication chains. For authentication trees, use the Scripted Decision Node to retrieve user attributes and session properties, or the Set Session Properties Node for session properties only.

Chapter 3

Deployment Configuration

Under Deployment, you can manage different configurations for AM server instances, and site configurations when using multiple AM server instances.

This section describes the following sets of properties:

- "Configuring Servers"
- "Configuring Sites"

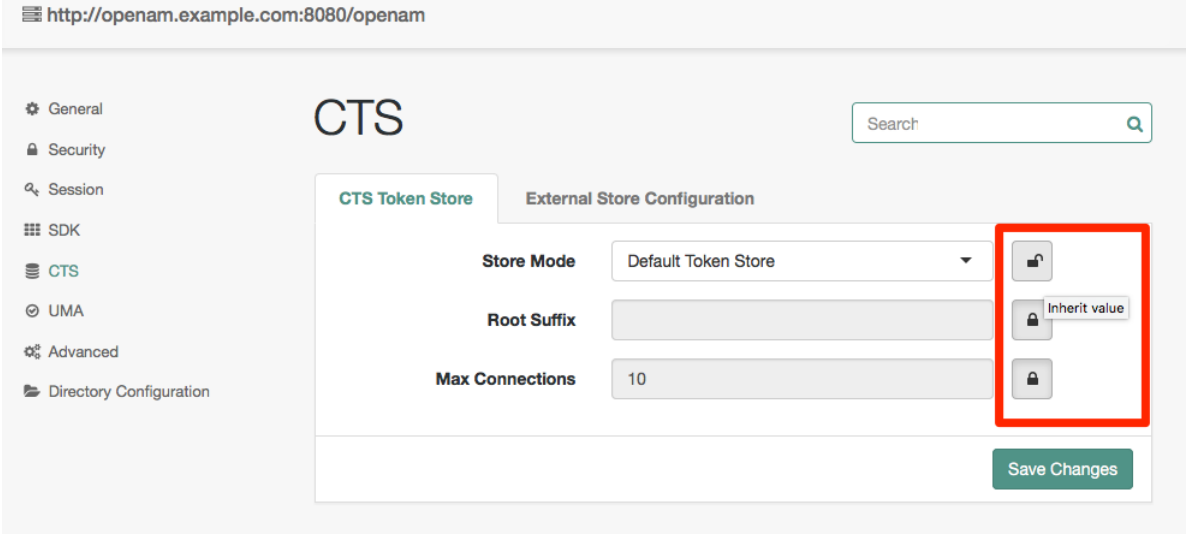
Configuring Servers

AM server properties reside in two places:

- The default configuration, under Configure > Server Defaults
- Per-server basis configuration, under Deployment > Servers > *Server Name*.

Default server properties are applied to all server instances, and can be overriden on a per-server basis. Changes to the value of a default server property are applied to all servers that are not overriding that property. The ability to set default properties and override them for an individual server allows you to keep a set of properties with identical configuration across the environment, while providing the flexibility to change properties on specific servers when required.

Inherited Properties



- A closed lock means the property is inherited from the defaults. To change an inherited value click on the lock, and the property will become localized for that server.
- An open lock means the property is localized for this server. To return to the inherited values, click on the lock.

The Advanced section also takes values from the defaults, but the properties do not have locks for inheritance. Instead, if you want to override a particular Advanced property value on a per-server basis, you need to add that property with its new value under Deployment > Servers > *Server Name* > Advanced.

Note

After changing server configurations, restart AM or the web application container where AM runs for the changes to take effect unless otherwise noted.

General Properties

The General page provides access to properties, such as site configuration, server base installation directory, default locale, debug levels, and other properties.

Site

The following properties are available under the Site tab:

Parent Site

Specifies the site the server belongs to. The drop-down list defaults to `[empty}` until there is at least one site created in the deployment.

Note

The Site tab is only available by navigating to Deployment > Servers > *Server Name* > General.

System

The following properties are available under the System tab:

Base installation directory

Specifies the directory where AM's configuration data and logs reside. For example, `/path/to/openam/`.

property: `com.iplanet.services.configpath`

Default Locale

Specifies the default locale of the UI pages when the client does not request a locale either by using the `locale` query string parameter or by setting the HTTP header, `Accept-Language`.

To set the locale when AM cannot find UI files for the requested locale, set the JVM platform locale instead.

Default: `en_US`

property: `com.iplanet.am.locale`

Notification URL

Specifies the URL of the notification service endpoint. For example, `https://openam.example.com:443/openam/notificationservice`

Default: `%SERVER_PROTO%://%SERVER_HOST%:%SERVER_PORT%/%SERVER_URI%/notificationservice`

property: `com.sun.identity.client.notification.url`

XML Validation

When enabled, AM validates any XML document it parses.

Default: `Off`

property: `com.iplanet.am.util.xml.validating`

Debugging

The following properties are available under the Debugging tab:

Debug Level

Specifies the log level shared across components for debug logging.

Changes to this property take effect immediately. No server restart is necessary.

Default: `Error`

property: `com.iplanet.services.debug.level`

Merge Debug Files

When enabled, AM writes debug log messages to a single file, `debug.out`. By default, AM writes a debug log per component.

Changes to this property take effect immediately. No server restart is necessary.

Default:`Off`

property: `com.iplanet.services.debug.mergeall`

Debug Directory

Specifies the path where AM writes debug logs. For example, `/path/to/openam/var/debug`

Changes to this property do not take effect until you restart the AM server.

Default: `%BASE_DIR%/%SERVER_URI%/var/debug`

property: `com.iplanet.services.debug.directory`

Mail Server

The following properties are available under the Mail Server tab:

Mail Server Host Name

Specifies the hostname of the SMTP server AM uses for sending email.

Default: `localhost`

property: `com.iplanet.am.smtphost`

Mail Server Port Number

Specifies the port of the SMTP server AM uses for sending email.

Default: `25`

property: `com.iplanet.am.smtpport`

Security Properties

Most security settings are inherited by default.

Encryption

The following properties are available under the Encryption tab:

Password Encryption Key

Specifies the encryption key for decrypting stored passwords.

The value of the `am.encryption.pwd` property must be the same for all deployed servers in a site. You can set the Password Encryption Key property at Deployment > Servers > *Server Name* > Security. Verify that all servers have the same setting for this property.

Example: `TF1Aue9c63bWTTY4mmZJeFYubJbNiSE3`

property: `am.encryption.pwd`

Encryption class

Specifies the default class used to handle encryption

Default: `com.iplanet.services.util.JCEEncryption`

property: `com.iplanet.security.encryptor`

Secure Random Factory Class

Specifies the class used to provide AM with cryptographically strong random strings. Possible values are the `com.iplanet.am.util.JSSSecureRandomFactoryImpl` class for JSS and the `com.iplanet.am.util.SecureRandomFactoryImpl` class for pure Java.

Default: `com.iplanet.am.util.SecureRandomFactoryImpl`

property: `com.iplanet.security.SecureRandomFactorImpl`

Validation

The following properties are available under the Validation tab:

Platform Low Level Comm. Max. Content Length

Specifies the maximum content length for an HTTP request.

Default: 16384

property: `com.iplanet.services.comm.server.pllrequest.maxContentLength`

Client IP Address Check

When enabled, AM checks client IP addresses when creating and validating SSO tokens.

Default: Disabled

property: `com.iplanet.am.clientIPCheckEnabled`

Cookie

The following properties are available under the Cookie tab:

Cookie Name

Specifies the cookie name AM uses to set a session handler ID during authentication.

Default: `iPlanetDirectoryPro`

property: `com.iplanet.am.cookie.name`

Secure Cookie

When enabled, AM generates secure cookies, which are only transmitted over an encrypted connection like HTTPS.

Default: Disabled

property: `com.iplanet.am.cookie.secure`

Encode Cookie Value

When enabled, AM URL-encodes the cookie values.

Default: Disabled

property: `com.iplanet.am.cookie.encode`

Key Store

The following properties are available under the Key Store tab:

Keystore File

Specifies the path to the AM keystore file, for example, `/path/to/openam/security/keystores/keystore.jceks`.

Default: `%BASE_DIR%/%SERVER_URI%/keystore.jceks`

property: `com.sun.identity.saml.xmlsig.keystore`

Keystore Type

Specifies the keystore type, for example `JKS`, `JCEKS`, `PKCS11`, or `PKCS12`.

This can be a custom keystore type, which must be supported by, and configured in, the local Java runtime environment.

Default: `JCEKS`

property: `com.sun.identity.saml.xmlsig.storetype`

Keystore Password File

Specifies the path to the password file for the keystore, for example, `/path/to/openam/security/secrets/default/.storepass`. The password contained in this file is in cleartext.

Default: `%BASE_DIR%/%SERVER_URI%/.storepass`

property: `com.sun.identity.saml.xmlsig.storepass`

Private Key Password File

Specifies the path to the password file for the private key aliases contained in the keystore, for example, `/path/to/openam/security/secrets/default/.keypass`. The password contained in this file is in cleartext.

Default: `%BASE_DIR%/%SERVER_URI%/.keypass`

property: `com.sun.identity.saml.xmlsig.keypass`

Certificate Alias

Leave the default `test` alias.

property: `com.sun.identity.saml.xmlsig.certalias`

Certificate Revocation List Caching

The following properties are available under the Certificate Revocation List Caching tab:

LDAP server host name

Specifies the hostname of the LDAP server where AM caches the certificate revocation list (CRL).

property: `com.sun.identity.crl.cache.directory.host`

LDAP server port number

Specifies the port number of the LDAP server where AM caches the certificate revocation list.

property: `com.sun.identity.crl.cache.directory.port`

SSL/TLS Enabled

When enabled, AM connects securely to the directory server holding the CRL cache. Ensure that AM trust the certificate from the LDAP server when enabling this option.

Default: Disabled

property: `com.sun.identity.crl.cache.directory.ssl`

LDAP server bind user name

Specifies the bind DN of the service account AM uses to authenticate to the LDAP server holding the CRL cache.

property: `com.sun.identity.crl.cache.directory.user`

LDAP server bind password

Specifies the bind password of the username set in the LDAP server bind user name property.

property: `com.sun.identity.crl.cache.directory.password`

LDAP search base DN

Specifies a valid Base DN for the LDAP search, such as `dc=example,dc=com`.

property: `com.sun.identity.crl.cache.directory.searchlocs`

Search Attributes

Specifies which DN component of issuer's subject DN is used to retrieve the CRL in the LDAP server, for example, `cn`.

property: `com.sun.identity.crl.cache.directory.searchattr`

Online Certificate Status Protocol Check

The following properties are available under the Online Certificate Status Protocol Check tab:

Check Enabled

When enabled, AM checks the revocation status of certificates using the Online Certificate Status Protocol (OCSP).

Default: Disabled

property: `com.sun.identity.authentication.ocspCheck`

Responder URL

Specifies the URL for the OCSP responder to contact about the revocation status of certificates.

property: `com.sun.identity.authentication.ocsp.responder.url`

Certificate Nickname

Specifies the nickname for the OCSP responder certificate set in the Responder URL property.

property: `com.sun.identity.authentication.ocsp.responder.nickname`

Object Deserialisation Class Whitelist

Whitelist

Specifies a list of classes that are considered valid when AM performs object deserialization operations.

Default: `com.iplanet.dpro.session.DNOrIPAddressListTokenRestriction, com.sun.identity.common.CaseInsensitiveHashMap,com.sun.identity.common.CaseInsensitiveHashSet, com.sun.identity.common.CaseInsensitiveKey, com.sun.identity.common.configuration.ServerConfigXML, com.sun.identity.common.configuration.ServerConfigXML$DirUserObject, com.sun.identity.common.configuration.ServerConfigXML$ServerGroup, com.sun.identity.common.configuration.ServerConfigXML$ServerObject, com.sun.identity.console.base.model.SMSubConfig, com.sun.identity.console.service.model.SMDescriptionData, com.sun.identity.console.service.model.SMDiscoEntryData, com.sun.identity.console.session.model.SMSessionData, com.sun.identity.console.user.model.UMUserPasswordResetOptionsData, com.sun.identity.shared.datastruct.OrderedSet,com.sun.xml.bind.util.ListImpl, com.sun.xml.bind.util.ProxyListImpl, java.lang.Boolean,java.lang.Integer, java.lang.Number,java.lang.StringBuffer, java.net.InetAddress,java.security.cert.Certificate, java.security.cert.Certificate$CertificateRep, java.util.ArrayList,java.util.Collections$EmptyMap, java.util.Collections$EmptySet, java.util.Collections$SingletonList, java.util.HashMap,java.util.HashSet, java.util.LinkedHashSet, java.util.Locale, org.forgerock.openam.authentication.service.protocol.RemoteCookie, org.forgerock.openam.authentication.service.protocol.RemoteHttpServletRequest, org.forgerock.openam.authentication.service.protocol.RemoteHttpServletResponse, org.forgerock.openam.authentication.service.protocol.RemoteServletRequest, org.forgerock.openam.authentication.service.protocol.RemoteServletResponse, org.forgerock.openam.authentication.service.protocol.RemoteSession, org.forgerock.openam.dpro.session.NoOpTokenRestriction`

property: `openam.deserialisation.classes.whitelist`

Session Properties

Session settings are inherited by default.

Session Limits

The following properties are available under the Sessions Limits tab:

Maximum Session Cache Size

Specifies the maximum number of sessions to cache in the AM server's internal session cache.

Default: `5000`

property: `org.forgerock.openam.session.service.access.persistence.caching.maxsize`

Invalidate Session Max Time

Specifies the time in minutes after which invalid CTS-based sessions are removed from the session table.

Default: `3` (minutes)

property: `com.iplanet.am.session.invalidsessionmaxtime`

Statistics

The following properties are available under the Statistics tab:

Logging Interval (in seconds)

Specifies the time in seconds AM delays between logging CTS-based session statistics. Any value lower than `5` is interpreted as `5` seconds.

Default: `60`

property: `com.iplanet.am.stats.interval`

State

Specifies whether to write statistics to a `File`, to the `Console`, or to turn recording `Off`.

Default: `File`

property: `com.iplanet.services.stats.state`

Directory

Specifies the path where AM writes the statistic files, for example, `/path/to/openam/var/stats`.

Default: `%BASE_DIR%/%SERVER_URI%/var/stats`

property: `com.iplanet.services.stats.directory`

Enable Host Lookup

When enabled, AM performs host lookup during CTS-based session logging.

Default: `Disabled`

property: `com.sun.am.session.enableHostLookUp`

Notification

The following properties are available under the Notification tab:

Notification Pool Size

Specifies the number of threads in the session change notification thread pool. Session notification applies to CTS-based sessions only.

Default: `10`

property: `com.iplanet.am.notification.threadpool.size`

Notification Thread Pool Threshold

Specifies the maximum number of tasks in the queue for serving session change notification threads. Session notification applies to CTS-based sessions only.

Default: `5000`

property: `com.iplanet.am.notification.threadpool.threshold`

Validation

The following properties are available under the Validation tab:

Case Insensitive client DN comparison

When enabled, AM performs case insensitive distinguished name comparison.

Default: `Enabled`

property: `com.sun.am.session.caseInsensitiveDN`

SDK Properties

Most SDK settings are inherited.

Data Store

The following properties are available under the Data Store tab:

Enable Datastore Notification

When enabled, AM uses data store notification. Otherwise, AM uses in-memory notification.

Changes to this property take effect immediately. No server restart is necessary.

Default: `Enabled`

property: `com.sun.identity.sm.enableDataStoreNotification`

Enable Directory Proxy

When enabled, AM accounts for the use of a directory proxy to access the directory server, for example, by enabling delegation privileges rather than ACIs for access control to the proxy.

Enable this option if you have deployed Directory Services as a directory proxy in front of a number of additional DS instances. For more information, see *Directory Proxy* in the *DS Installation Guide*.

Default: `Disabled`

property: `com.sun.identity.sm.ldap.enableProxy`

Notification Pool Size

Specifies the size of the thread pool used to send notifications. A value of `1` causes notifications to be processed sequentially, avoiding any potential out-of-order conditions. In production, where configuration is unlikely to change often, keeping the default of `1` is recommended.

Default: `1`

property: `com.sun.identity.sm.notification.threadpool.size`

Event Service

The following properties are available under the Event Service tab:

Number of retries for Event Service connections

Specifies the maximum number of attempts to reestablish event service connections.

Default: `3`

property: `com.iplanet.am.event.connection.num.retries`

Delay between Event Service connection retries

Specifies the time in milliseconds between attempts to reestablish entry service connections.

Default: `3000`

property: `com.iplanet.am.event.connection.delay.between.retries`

Error codes for Event Service connection retries

Specifies the LDAP error codes for which AM retries rather than returning failure.

Default: `80,81,91`

property: `com.iplanet.am.event.connection.ldap.error.codes.retries`

Disabled Event Service Connection

Specifies which persistent search connections AM can disable. Any connection that is not specified as disabled is enabled. Possible values are:

- `aci`. Obtain notification changes to the `aci` attribute.
- `um`. Obtain notification changes in AM's user store. For example, modifying a password.
- `sm`. Obtain notification changes in AM's configuration store. For example, modifying a realm.

Multiple values should be separated with a comma `,`.

Default: `aci,um`

property: `com.sun.am.event.connection.disable.list`

LDAP Connection

The following properties are available under the LDAP Connection tab:

Number of retries for LDAP Connection

Specifies the maximum number of attempts to reestablish LDAP connections.

Default: `3`

property: `com.iplanet.am.ldap.connection.num.retries`

Delay between LDAP connection retries

Specifies the time, in milliseconds, between attempts to reestablish LDAP connections.

Default: `1000`

property: `com.iplanet.am.ldap.connection.delay.between.retries`

Error Codes for LDAP connection retries

Specifies the LDAP error codes for which AM retries rather than returning failure.

Default: `80,81,91`

property: `com.iplanet.am.ldap.connection.ldap.error.codes.retries`

Caching and Replica

The following properties are available under the Caching and Replica tab:

SDK Caching Max. Size

Specifies the cache size used when SDK caching is enabled. The size should be an integer greater than `0`, or the default size of `10000` will be used.

Changes to this property clear the contents of the cache. No server restart is necessary.

Default: `10000`

property: `com.iplanet.am.sdk.cache.maxSize`

SDK Replica Retries

Specifies the maximum number of attempts to retry when an entry not found error is returned to the SDK.

Changes to this property take effect immediately. No server restart is necessary.

Default: `0`

property: `com.iplanet.am.replica.num.retries`

Delay between SDK Replica Retries

Specifies the time in milliseconds between attempts to retrieve entries through the SDK.

Changes to this property take effect immediately. No server restart is necessary.

Default: `1000`

property: `com.iplanet.am.replica.delay.between.retries`

Time To Live Configuration

The following properties are available under the Time to Live Configuration tab:

Cache Entry Expiration Enabled

When disabled, cache entries expire based on the User Entry Expiration Time property.

Default: `Disabled`

property: `com.iplanet.am.sdk.cache.entry.expire.enabled`

User Entry Expiration Time

Specifies the time in minutes for which user entries remain valid in cache after their last modification. When AM accesses a user entry that has expired, it reads the entry from the directory server instead of from the cache.

Default: `15`

property: `com.iplanet.am.sdk.cache.entry.user.expire.time`

Default Entry Expiration Time

Specifies the time in minutes for which non-user entries remain valid in cache after their last modification. When AM accesses a non-user entry that has expired, it reads the entry from the directory server instead of from the cache.

Default: `30`

property: `com.iplanet.am.sdk.cache.entry.default.expire.time`

CTS Properties

The Core Token Service (CTS) does not need to be configured in the same LDAP storage as the configuration store. The CTS can instead be configured on its own external directory server. There are some specific requirements for indexing and replication which need to be accounted for. In particular, WAN replication is an important consideration which needs to be handled carefully for optimum performance.

You may also choose to set advanced properties related to token size, including `com.sun.identity.session.repository.enableEncryption`, `com.sun.identity.session.repository.enableCompression`, and `com.sun.identity.session.repository.enableAttributeCompression`. For more information about these three properties, see "Advanced Properties".

CTS Token Store

The following properties are available under the CTS Token Store tab:

Store Mode

Specifies whether AM stores CTS tokens in the default token store or in an external token store.

CTS tokens are stored in the same data store used for the AM configuration when you specify the `Default Token Store` option. When specifying this option, you can only configure the properties available under the CTS Token Store tab.

You can separate the CTS store from the AM configuration on different external servers by selecting the `External Token Store` option. When specifying this option, you can configure the properties available under both the CTS Token Store and the External Store Configuration tabs.

Root Suffix

For either default or external token stores, specifies the base DN for CTS storage information in LDAP format, such as `cn=cts,ou=famrecords,ou=openam-session,ou=tokens`. The Root Suffix specifies a database that can be maintained and replicated separately from the standard user data store.

Max Connections

Specifies the maximum number of remote connections to the external data store. For affinity deployments, this property specifies the maximum number of remote connections to each directory server in the connection string.

Default: `10`

For suggested settings, see "Tuning CTS Store LDAP Connections" in the *Maintenance Guide*.

Page Size

The number of results per page returned from the underlying CTS 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 the result set size divided by the page size.

Increasing the page size results in fewer round trips to the CTS datastore when retrieving large result sets.

To return all results and disable pagination, set to `0`.

Default: `0`

VLV Page Size

The number of results per page returned from the underlying CTS datastore when using virtual list views (VLVs). Larger values will result in fewer round trips to the datastore when retrieving large result sets, and VLVs are enabled on the datastore.

For more information on VLVs, see Virtual List View Index in the *DS 7.1 Configuration Guide*

Default: `10`

External Store Configuration

AM honors the following properties when `External Token Store` is selected under the CTS Token Store tab:

SSL/TLS Enabled

When enabled, AM accesses the external directory service using StartTLS or SSL.

Connection String(s)

Specifies the ordered list of connection strings for external DS servers. The format is `HOST:PORT[|SERVERID[|SITEID]]`, where `HOST:PORT` are the LDAP server and its port. `SERVERID` and `SITEID` are optional parameters to specify an AM instance that prioritizes the particular connection. This does not exclude other AM instances from using that connection, although they must have no remaining priority connections available to them before they use it.

When a failed DS server becomes available again, AM instances create new connections to it based on the order specified in the list.

Examples for active/passive deployments:

`cts-dj1.example.com:389,cts-dj2.example.com:389`

Every AM instance accesses `cts-dj1.example.com:389` for all CTS operations. If it goes down, they access `cts-dj2.example.com:389`.

Every instance will open new connections to `cts-dj1.example.com:389` when it becomes available.

`cts-dj1.example.com:389|1|1,cts-dj2.example.com:389|2|1`

Server 1 site 1 gives priority to `cts-dj1.example.com:389`. Server 2 site 1 gives priority to `cts-dj2.example.com:389`. Any server not specified accesses the first server on the list, while it is available.

If `cts-dj1.example.com:389` goes down, server 1 site 1 accesses `cts-dj2.example.com:389`. Any server not specified access the second server on the list.

If `cts-dj2.example.com:389` goes down, server 2 site 1 accesses `cts-dj1.example.com:389`. Any server not specified still accesses the first server on the list.

Server 1 site 1 and any server not specified will open new connections to `cts-dj1.example.com:389` when it becomes available. Only server 2 site 1 will open new connections to `cts-dj2.example.com:389` when it becomes available.

`cts-dj1.example.com:389|1|1,cts-dj2.example.com:389|1|1,cts-dj3.example.com:389|1|2`

Server 1 site 1 gives priority to `cts-dj1.example.com:389`. Any server not specified accesses the first server on the list, while it is available.

If `cts-dj1.example.com` goes down, server 1 site 1 accesses `cts-dj2.example.com:389`. Any server not specified accesses the second server on the list.

If both `cts-dj1.example.com` and `cts-dj2.example.com` go down, server 1 site 1 accesses `cts-dj3.example.com:389` in site 2. Any server not specified accesses the third server on the list.

Server 1 site 1 and any server not specified will open new connections to any server in site 1 when they become available, with `cts-dj1.example.com` being the preferred server.

Example for affinity deployments:

`cts-dj1.example.com:389,cts-dj2.example.com:389,cts-dj3.example.com:389,cts-dj4.example.com:389`

Access CTS tokens from one of the four servers listed in the connection string. For any given CTS token, AM determines the token's affinity for one of the four servers, and always accesses the token from that same server. Tokens are distributed equally across the four servers.

Login Id

Specifies the user, in DN format, needed to authenticate to the external data store. The user needs sufficient privileges to read and write to the root suffix of the external data store.

Password

Specifies the password associated with the login ID.

Heartbeat

Specifies how often AM should send a heartbeat request to the directory server to ensure that the connection does not remain idle, in seconds. Configure the heartbeat to ensure that network hardware, such as routers and firewalls, does not drop the connection between AM and the directory server.

Default: `10`

Affinity Enabled

When enabled, specifies whether to access the CTS token store by using multiple directory instances in an affinity deployment rather than a single master directory instance using an active/passive deployment.

When you enable this option, you must ensure that the value of the Connection String(s) property is identical for every server in multi-server deployments.

Default: Disabled

UMA Properties

UMA server settings are inherited by default.

UMA Resource Store

The following settings appear on the UMA Resource Store tab:

Store Mode

Specifies the data store where AM stores UMA tokens. Possible values are:

- `Default Token Store`: AM stores UMA tokens in the configuration data store.

- `External Token Store`: AM stores UMA tokens in an external data store.

Root Suffix

Specifies the base DN for storage information in LDAP format, such as `dc=uma-resources,dc=example,dc=com`.

Max Connections

Specifies the maximum number of connections to the data store.

External UMA Resource Store Configuration

AM honors the following properties when `External Token Store` is selected under the Resource Sets Store tab:

SSL/TLS Enabled

When enabled, AM uses SSL or TLS to connect to the external data store. Make sure AM trusts the data store's certificate when using this option.

Connection String(s)

Specifies an ordered list of connection strings for external data stores. The format is `HOST:PORT[|SERVERID[|SITEID]]`, where `HOST:PORT` specify the FQDN and port of the data store, and `SERVERID` and `SITEID` are optional parameters that let you prioritize the particular connection when used by the specified node(s).

Multiple connection strings must be comma-separated, for example, `uma-ldap1.example.com:389|1|1, uma-ldap2.example.com:389|2|1`.

See the entry for Connection String(s) in "CTS Properties" for more syntax examples.

Login Id

Specifies the username AM uses to authenticate to the data store. For example, `uid=am-uma-bind-account,ou=admins,dc=uma,dc=example,dc=com`. This user must be able to read and write to the root suffix of the data store.

Password

Specifies the password associated with the login ID property.

Heartbeat

Specifies, in seconds, how often AM should send a heartbeat request to the data store to ensure that the connection does not remain idle.

Default: `10`

UMA Audit Store

The following settings appear on the UMA Audit Store tab:

Store Mode

Specifies the data store where AM stores audit information generated when users access UMA resources. Possible values are:

- `Default Token Store`: AM stores UMA audit information in the configuration data store.
- `External Token Store`: AM stores UMA audit information in an external data store.

Root Suffix

Specifies the base DN for storage information in LDAP format, such as `dc=uma-audit,dc=example,dc=com`.

Max Connections

Specifies the maximum number of connections to the data store.

External UMA Audit Store Configuration

AM honors the following properties when `External Token Store` is selected under the UMA Audit Store tab:

SSL/TLS Enabled

When enabled, AM uses SSL or TLS to connect to the external data store. Make sure AM trusts the data store's certificate when using this option.

Connection String(s)

Specifies an ordered list of connection strings for external data stores. The format is `HOST:PORT[|SERVERID[|SITEID]]`, where `HOST:PORT` specify the FQDN and port of the data store, and `SERVERID` and `SITEID` are optional parameters that let you prioritize the particular connection when used by the specified node(s).

Multiple connection strings must be comma-separated, for example, `uma-ldap1.example.com:389|1|1, uma-ldap2.example.com:389|2|1`.

See the entry for Connection String(s) in "CTS Properties" for more syntax examples.

Login Id

Specifies the username AM uses to authenticate to the data store. For example, `uid=am-uma-bind-account,ou=admins,dc=uma,dc=example,dc=com`. This user must be able to read and write to the root suffix of the data store.

Password

Specifies the password associated with the login ID property.

Heartbeat

Specifies, in seconds, how often AM should send a heartbeat request to the data store to ensure that the connection does not remain idle.

Default: `10`

Pending Requests Store

The following settings appear on the Pending Requests Store tab:

Store Mode

Specifies the data store where AM stores pending requests to UMA resources. Possible values are:

- `Default Token Store`: AM stores UMA pending requests in the configuration data store.
- `External Token Store`: AM stores UMA pending requests in an external data store.

Root Suffix

Specifies the base DN for storage information in LDAP format, such as `dc=uma-pending,dc=forgerock,dc=com`.

Max Connections

Specifies the maximum number of connections to the data store.

External Pending Requests Store Configuration

AM honors the following properties when `External Token Store` is selected under the Pending Requests Store tab:

SSL/TLS Enabled

When enabled, AM uses SSL or TLS to connect to the external data store. Make sure AM trusts the data store's certificate when using this option.

Connection String(s)

Specifies an ordered list of connection strings for external data stores. The format is `HOST:PORT[|SERVERID[|SITEID]]`, where `HOST:PORT` specify the FQDN and port of the data store, and `SERVERID` and `SITEID` are optional parameters that let you prioritize the particular connection when used by the specified node(s).

Multiple connection strings must be comma-separated, for example, `uma-ldap1.example.com:389|1|1, uma-ldap2.example.com:389|2|1`.

See the entry for Connection String(s) in "CTS Properties" for more syntax examples.

Login Id

Specifies the username AM uses to authenticate to the data store. For example, `uid=am-uma-bind-account,ou=admins,dc=uma,dc=example,dc=com`. This user must be able to read and write to the root suffix of the data store.

Password

Specifies the password associated with the login ID property.

Heartbeat

Specifies, in seconds, how often AM should send a heartbeat request to the data store to ensure that the connection does not remain idle.

Default: `10`

UMA Resource Labels Store

The following settings appear on the UMA Resource Labels Store tab:

Store Mode

Specifies the data store where AM stores user-created labels used for organizing UMA resources. Possible values are:

- `Default Token Store`: AM stores user-created labels in the configuration data store.
- `External Token Store`: AM stores user-created labels in an external data store.

Root Suffix

Specifies the base DN for storage information in LDAP format, such as `dc=uma-resources-labels,dc=forgerock,dc=com`.

Max Connections

Specifies the maximum number of connections to the data store.

External UMA Resource Labels Store Configuration

AM honors the following properties when `External Token Store` is selected under the UMA Resource Labels Store tab.

SSL/TLS Enabled

When enabled, AM uses SSL or TLS to connect to the external data store. Make sure AM trusts the data store's certificate when using this option.

Connection String(s)

Specifies an ordered list of connection strings for external data stores. The format is `HOST:PORT[|SERVERID[|SITEID]]`, where `HOST:PORT` specify the FQDN and port of the data store, and `SERVERID` and `SITEID` are optional parameters that let you prioritize the particular connection when used by the specified node(s).

Multiple connection strings must be comma-separated, for example, `uma-ldap1.example.com:389|1|1, uma-ldap2.example.com:389|2|1`.

See the entry for Connection String(s) in "CTS Properties" for more syntax examples.

Login Id

Specifies the username AM uses to authenticate to the data store. For example, `uid=am-uma-bind-account,ou=admins,dc=uma,dc=example,dc=com`. This user must be able to read and write to the root suffix of the data store.

Password

Specifies the password associated with the login ID property.

Heartbeat

Specifies, in seconds, how often AM should send a heartbeat request to the data store to ensure that the connection does not remain idle.

Default: `10`

Directory Configuration Properties

Configure connection settings and additional LDAP directory server instances by navigating to Deployment > Servers > *Server Name* > Directory Configuration.

Directory Configuration

The following properties are available under the Directory Configuration tab:

Minimum Connection Pool

Sets the minimum number of connections in the pool.

Changes to this property take effect immediately. No server restart is necessary.

Maximum Connection Pool

Sets the maximum number of connections in the pool.

Changes to this property take effect immediately. No server restart is necessary.

Bind DN

Sets the bind DN of the service account AM uses to connect to the configuration directory servers.

Changes to this property take effect immediately. No server restart is necessary.

Bind Password

Set the bind password to connect to the configuration directory servers.

Changes to this property take effect immediately. No server restart is necessary.

Server

In the LDAP connection table, edit existing LDAP connections by selecting the pen icon to the right of the row you want to modify. To add a new entry, fill the NAME, HOST NAME, PORT NUMBER and CONNECTION TYPE columns using the following hints:

- **NAME**. The name of the LDAP connection.
- **HOST NAME**. The FQDN of the LDAP server.
- **PORT NUMBER**. The port number to connect to the LDAP server.
- **CONNECTION TYPE**. Whether the connection between the LDAP server and AM is `SIMPLE` (unsecured) or `SSL` (secured).

Advanced Properties

Each server has a list of advanced properties that can be modified by navigating to Deployment > Servers > *Server Name* > Advanced. For a list of inherited advanced properties relevant to all servers, navigate to Configure > Server Defaults > Advanced.

`bootstrap.file`

File that contains the path to the AM configuration folder. By default, the `.openamcfg` directory is created in the home directory of the user that runs the web container. For example, `/usr/local/.openamcfg/AMConfig_usr_local_apache-tomcat-8.0.35_webapps_openam_`.

`com.forgerock.openam.dj.backendType`

The backend type for the embedded DS server.

Default: `je`

`com.iplanet.am.cookie.c66Encode`

Properly URL encode session tokens.

Default: `true`

`com.iplanet.am.daemons`

Modules for which to open daemons at AM startup.

Default: `securid`

`com.iplanet.am.directory.ssl.enabled`

Whether to connect to the configuration directory server over LDAPS.

Default: `false`

`com.iplanet.am.installdir`

AM Configuration and log file location.

Default: `~/openam/`, such as `~/openam`

`com.iplanet.am.jssproxy.checkSubjectAltName`

When using JSS or JSSE, check whether the name values in the `SubjectAltName` certificate match the server FQDN.

Default: `false`

`com.iplanet.am.jssproxy.resolveIPAddress`

When using JSS or JSSE, check that the IP address of the server resolves to the host name.

Default: `false`

`com.iplanet.am.jssproxy.SSLTrustHostList`

When using JSS or JSSE, comma-separated list of server FQDNs to trust if they match the certificate CN, even if the domain name is not correct.

`com.iplanet.am.jssproxy.trustAllServerCerts`

When using JSS or JSSE, set to `true` to trust whatever certificate is presented without checking.

Default: `true`

`com.iplanet.am.lbcookie.name`

Used with sticky load balancers that can inspect the cookie value.

Default: `amlbcookie`

`com.iplanet.am.lbcookie.value`

Used with sticky load balancers that can inspect the cookie value. The value of this property defaults to the unique AM server ID, although you can set your own unique value.

To improve AM server performance, keep the value of the cookie set to the AM server ID when using Web Agents.

If you have replaced the value of the this property and you need to match the AM server URLs with their corresponding server IDs, query the `global-config/servers` endpoint. For example:

```
$ curl \
--header 'Accept: application/json' \
--header "iPlanetDirectoryPro: AQIC5...NDU1*" \
--header  "Accept-API-Version: resource=1.0, protocol=2.1" \
'https://openam.example.com:8443/openam/json/global-config/servers?_queryFilter=true'
      {
    "result": [
        {
            "_id": "01",
            "_rev": "-1541617246",
            "siteName": null,
            "url": "https://openam.example.com:8443/openam"
        }
    ],
    "resultCount": 1,
    "totalPagedResults": -1,
    "totalPagedResultsPolicy": "NONE"
}
```

In the example above, the server ID for server `https://openam.example.com:8443/openam` is `01`.

Default: `01`

`com.iplanet.am.pcookie.name`

Persistent cookie name.

Default: `DProPCookie`

`com.iplanet.am.profile.host`

Not used

Default: *server-host*, such as `openam.example.com`

`com.iplanet.am.profile.port`

Not used

Default: *server-port*, such as `8080` or `8443`

`com.iplanet.am.sdk.caching.enabled`

Enables caching for configuration data and user data. Refer to "Overall Server Cache Settings" in the *Maintenance Guide* for important information about this property.

Changes to this property take effect immediately. No server restart is necessary.

Default: `true`

`com.iplanet.am.session.agentSessionIdleTime`

Time in *minutes* after which a web or Java agent's CTS-based session expires. Note that this setting is ignored when AM creates a client-based session for a web or Java agent.

Default: `1440` (session expires after one day). You can set this property to `0` (session never expires), or any integer higher than `30` (no maximum limit).

`com.iplanet.am.session.client.polling.enable`

Whether client applications such as web or Java agents poll for CTS-based session changes. If `false`, then client applications register listeners for notifications about changes to CTS-based sessions.

Default: `false`

`com.iplanet.am.session.client.polling.period`

If client applications poll for changes, number of seconds between polls.

Default: `180`

`com.iplanet.am.session.httpSession.enabled`

Create an `HttpSession` for users on successful authentication.

Default: `true`

`com.iplanet.security.SSLSocketFactoryImpl`

SSL socket factory implementation used by AM.

Default: `com.sun.identity.shared.ldap.factory.JSSESocketFactory`, uses a pure Java provider

`com.sun.embedded.replicationport`

Replication port for the embedded DS server.

Default: `8989`

`com.sun.embedded.sync.servers`

This property applies to multi-server AM deployments that use the embedded DS store.

When this property is set to `on`, AM servers check during startup to determine whether the replication settings for the embedded store are consistent with the number of servers in the site. If they are not consistent, AM reconfigures replication to match the existing number of servers in the site.

> **Note**
>
> Set this property on a per-server basis by navigating to Deployment > Servers > *Server Name* > Advanced, rather than globally under Configure > Server Defaults.

Default: `on`

`com.sun.identity.am.cookie.check`

Whether to check for cookie support in the user agent, and if not to return an error.

Default: `false`

`com.sun.identity.appendSessionCookieInURL`

Whether to append the session cookie to URL for a zero page session.

Default: `true`

`com.sun.identity.auth.cookieName`

Cookie used by the AM authentication service to handle the authentication process.

Default: `AMAuthCookie`

`com.sun.identity.authentication.client.ipAddressHeader`

Set the name of the HTTP header that AM can examine to learn the client IP address when requests go through a proxy or load balancer. (When requests go through an HTTP proxy or load balancer, checking the IP address on the request alone returns the address of the proxy or load balancer rather than that of the client.) AM must be able to trust the proxy or load balancer to set the client IP address correctly in the header specified.

Example: `com.sun.identity.authentication.client.ipAddressHeader=X-Forwarded-For`

`com.sun.identity.authentication.multiple.tabs.used`

Whether to allow users to open many browser tabs to the login page at the same time without encountering an error.

Default: `false`

`com.sun.identity.authentication.setCookieToAllDomains`

Whether to allow multiple cookie domains.

Default: `true`

`com.sun.identity.authentication.special.users`

List of special users always authenticated against the local directory server.

Default: `cn=dsameuser,ou=DSAME Users,dc=openam,dc=forgerock,dc=org`

`com.sun.identity.authentication.super.user`

Identifies an administrative user that replaces the `amAdmin` user. For example, `uid=superroot,ou=people,dc=example,dc=com`.

You must manually create a user account for the new administrative user in the configuration data store that has the same privileges as the `uid=admin` user.

Warning

The `amAdmin` account is "hard-coded" in the source of several files. The code in these files may affect the functionality of a top-level administrative user with a name other than `amAdmin`.

Default: `uid=amAdmin,ou=People,dc=openam,dc=forgerock,dc=org`

`com.sun.identity.authentication.uniqueCookieName`

When cookie hijacking protection is configured, name of the cookie holding the URL to the AM server that authenticated the user.

Default: `sunIdentityServerAuthNServer`

`com.sun.identity.client.notification.url`

Notification service endpoint for clients such as web and Java agents.

Default: *`server-protocol://server-host:server-port/server-uri`*`/notificationservice`, such as `https://openam.example.com:8443/openam/notificationservice`

`com.sun.identity.common.systemtimerpool.size`

Number of threads in the shared system timer pool used to schedule operations such as session timeout.

Default: `3`

`com.sun.identity.cookie.httponly`

When set to `true`, mark cookies as HTTPOnly to prevent scripts and third-party programs from accessing the cookies.

Note that this configuration option is used only in non-UI deployments. The UI cannot set the HttpOnly name in a cookie.

Default: `false`

`com.sun.identity.cookie.samesite`

Configures support for applying *SameSite* cookie rules, as per internet-draft Cookies: HTTP State Management Mechanism.

Available settings are as follows:

`strict`

Requests originating from different domains will not have cookies sent with them.

When this mode is enabled, any AM functionality that relies on requests being redirected back to the AM instance may not operate correctly. For example, OAuth 2.0 flows and SAML federation may not operate correctly if AM cannot access the required cookies.

`lax`

Cookies received from different domains cannot be accessed, unless the request is using a *top-level* request and uses a "safe" HTTP method, such as GET, HEAD, OPTIONS, and TRACE.

`off`

No restrictions on the domain of cookies is applied. This is the default setting.

Important

You must disable *SameSite* support if any of the following is true:

- You have set `Access-Control-Allow-Credentials=true` in your CORS configuration. For more information on configuring CORS in AM, see "Configuring CORS Support" in the *Security Guide*.
- You are using SAML HTTP-POST bindings. For example, IDP-initiated single logout (SLO) functionality will not operate correctly if *SameSite* support is enabled, as the `iPlanetDirectoryPro` cookie would not be accessible in cross-domain POST requests. For more information on SAML single logout, see "*Implementing SSO and SLO*" in the *SAML v2.0 Guide*.

Default: `off`

`com.sun.identity.enableUniqueSSOTokenCookie`

If `true`, then AM is using protection against cookie hijacking.

Default: `false`

`com.sun.identity.jss.donotInstallAtHighestPriority`

Whether JSS should take priority over other providers.

Default: `true`

`com.sun.identity.monitoring`

Whether monitoring is active for AM.

Default: `off`

`com.sun.identity.monitoring.local.conn.server.url`

URL for local connection to the monitoring service.

Default: `service:jmx:rmi://`

`com.sun.identity.password.deploymentDescriptor`

Internal property used by AM.

Default: *server-uri*, such as `openam`

`com.sun.identity.policy.Policy.policy_evaluation_weights`

Weights of the cost of evaluating policy subjects, rules, and conditions. Evaluation is in order of heaviest weight to lightest weight.

Default: `10:10:10`, meaning evaluation of rules, then conditions, then subjects

`com.sun.identity.policy.resultsCacheMaxSize`

Maximum number of policy decisions AM caches.

Default: `10000`

`com.sun.identity.security.checkcaller`

Whether to perform a Java security permissions check for AM.

Default: `false`

`com.sun.identity.server.fqdnMap`

Enables virtual hosts, partial hostname and IP address. Maps invalid or virtual name keys to valid FQDN values for proper redirection.

To map `myserver` to `myserver.example.com`, set `com.sun.identity.server.fqdnMap[myserver]=myserver.example.com`.

`com.sun.identity.session.repository.enableAttributeCompression`

For additional compression of CTS token JSON binaries, beyond GZip, if desired.

Default: `false`

`com.sun.identity.session.repository.enableCompression`

For GZip-based compression of CTS tokens, if desired.

Default: `false`

`com.sun.identity.session.repository.enableEncryption`

Enables tokens to be encrypted when stored.

Multi-instance deployments require consistent use of this property, which should be configured under Configure > Server Defaults > Advanced.

The `am.encryption.pwd` property must also be the same for all deployed instances. You can set the Password Encryption Key property under Deployment > Servers > *Server Name* > Security. Verify that all servers have the same setting for this property.

Default: `false`

`com.sun.identity.sm.cache.enabled`

Enables service configuration caching. See "Overall Server Cache Settings" in the *Maintenance Guide* for important information about this property.

Changes to this property take effect immediately. No server restart is necessary.

Default: `true`

`com.sun.identity.sm.cache.ttl`

When service configuration caching time-to-live is enabled, this sets the time to live in minutes.

Changes to this property take effect immediately. No server restart is necessary.

Default: `30`

`com.sun.identity.sm.cache.ttl.enable`

If service configuration caching is enabled, whether to enable a time-to-live for cached configuration.

Changes to this property take effect immediately. No server restart is necessary.

Default: `false`

`com.sun.identity.sm.flatfile.root_dir`

File system directory to hold file-based representation of AM configuration.

Default: `/path/to/openam/`

`com.sun.identity.sm.sms_object_class_name`

Class used to read and write AM service configuration entries in the directory.

Default: `com.sun.identity.sm.ldap.SMSEmbeddedLdapObject`

`com.sun.identity.url.readTimeout`

Used to set the read timeout in milliseconds for HTTP and HTTPS connections to other servers.

Default: `30000`

`com.sun.identity.urlchecker.dorequest`

Whether to perform an HTTP GET on `com.sun.identity.urlchecker.targeturl` as a health check against another server in the same site.

If set to `false`, then AM only checks the Socket connection, and does not perform an HTTP GET.

If each AM server runs behind a reverse proxy, then the default setting of `true` means the health check actually runs against the AM instance, rather than checking only the Socket to the reverse proxy.

Default: `true`

`com.sun.identity.urlchecker.targeturl`

URL to monitor when `com.sun.identity.urlchecker.dorequest` is set to `true`.

Default: URL to the `/openam/namingservice` endpoint on the remote server

`com.sun.identity.urlconnection.useCache`

Whether to cache documents for HTTP and HTTPS connections to other servers.

Default: `false`

`com.sun.identity.webcontainer`

Name of the web container to correctly set character encoding, if necessary.

Default: `WEB_CONTAINER`

`console.privileged.users`

Used to assigned privileged console access to particular users. Set to a `|` separated list of users' Universal IDs, such as `console.privileged.users=uid=demo,ou=user,dc=openam,dc=forgerock,dc=org|uid=demo2,ou=user,dc=openam,dc=forgerock,dc=org`.

`openam.auth.destroy_session_after_upgrade`

Where to destroy the old session after a session is successfully upgraded.

Default: `true`

`openam.auth.distAuthCookieName`

Cookie used by the AM distributed authentication service to handle the authentication process.

Default: `AMDistAuthCookie`

`openam.auth.session_property_upgrader`

Class that controls which session properties are copied during session upgrade, where default is to copy all properties to the upgraded session.

Default: `org.forgerock.openam.authentication.service.DefaultSessionPropertyUpgrader`

`openam.auth.version.header.enabled`

The X-DSAMEVersion http header provides detailed information about the version of AM currently running on the system, including the build and date/time of the build. AM will need to be restarted once this property is enabled.

Default: `false`

`openam.authentication.ignore_goto_during_logout`

Whether to ignore the `goto` query string parameter on logout, instead displaying the logout page.

Default: `false`

`openam.cdm.default.charset`

Character set used for globalization.

Default: `UTF-8`

`openam.forbidden.to.copy.headers`

Comma-separated list of HTTP headers not to copy when the distributed authentication server forwards a request to another distributed authentication server.

Default: `connection`

`openam.forbidden.to.copy.request.headers`

Comma-separated list of HTTP headers not to copy when the distributed authentication server forwards a request to another distributed authentication server.

Default: `connection`

`openam.private.key.jwt.encryption.algorithm.whitelist`

Comma-separated list of encryption algorithms that the OpenID Connect clients of the Social Identity Provider service can configure in the Private Key JWT Encryption Algorithm field.

For a list of algorithms that AM supports, see the JSON Web Algorithms (JWA) internet draft.

For more information, see the Social Identity Provider service client configuration reference.

Unrecognized or unsupported algorithms will be saved, but not exposed in the Private Key JWT Encryption Algorithm field.

This property is hot-swappable.

Default: `RSA-OAEP,RSA-OAEP-256,ECDH-ES`

`openam.retained.http.headers`

Comma-separated list of HTTP headers to copy to the forwarded response when the server forwards a request to another server.

Requests are forwarded when the server receiving the request is not the server that originally initiated authentication. The server that originally initiated authentication is identified by a cookie.

When the distributed authentication service (DAS) is in use, then the cookie is the `AMDistAuthCookie` that identifies the DAS server by its URL.

When authentication is done directly on AM, then the cookie is the `AMAuthCookie` that holds a session ID that identifies the AM server.

On subsequent requests the server receiving the request checks the cookie. If the cookie identifies another server, the current server forwards the request to that server.

If a header such as `Cache-Control` has been included in the list of values for the property `openam.retained.http.request.headers` and the header must also be copied to the response, then add it to the list of values for this property.

Example: `openam.retained.http.headers=X-DSAMEVersion,Cache-Control`

Default: `X-DSAMEVersion`

`openam.retained.http.request.headers`

Comma-separated list of HTTP headers to copy to the forwarded request when the server forwards a request to another server.

Requests are forwarded when the server receiving the request is not the server that originally initiated authentication. The server that originally initiated authentication is identified by a cookie.

When the distributed authentication service (DAS) is in use, then the cookie is the `AMDistAuthCookie` that identifies the DAS server by its URL.

When authentication is done directly on AM, then the cookie is the `AMAuthCookie` that holds a session ID that identifies the AM server.

On subsequent requests the server receiving the request checks the cookie. If the cookie identifies another server, the current server forwards the request to that server.

When configuring the distributed authentication service, or when a reverse proxy is set up to provide the client IP address in the `X-Forwarded-For` header, if your deployment includes multiple AM servers, then this property must be set to include the header.

Example: `openam.retained.http.request.headers=X-DSAMEVersion,X-Forwarded-For`

AM copies the header when forwarding a request to the authoritative server where the client originally began the authentication process, so that the authoritative AM server receiving the forwarded request can determine the real client IP address.

In order to retain headers to return in the response to the AM server that forwarded the request, use the property `openam.retained.http.headers`.

Default: `X-DSAMEVersion`

`openam.session.case.sensitive.uuid`

Whether universal user IDs are considered case sensitive when matching them.

Default: `false`

`org.forgerock.allow.http.client.debug`

Specifies whether AM can output logging at the `Message` level for the `org.apache.http.wire` and `org.apache.http.headers` logging appenders.

Possible values are:

- `true`. The appenders' debug log level can take the same value as AM's, even `Message`.

  Caution

  The appenders can log cleartext passwords or sensitive information related to client interactions. For example, scripted authentication or STS transactions.

  Enable this property for debugging purposes only when required.

- `false`. The appender's debug log level is always `warning`, unless debug is disabled.

You can also set this property as a JVM option in the container where AM runs.

Default: `false`

`org.forgerock.openam.http.ssl.connection.manager`

Specifies the class that implements the `org.forgerock.openam.http.SslConnectionManager` interface, which controls both keystore and truststore settings, as well as hostname verification.

If the container in which AM runs is configured with the `java.protocol.handler.pkgs` property set, then ensure this property is set to `com.sun.identity.protocol.AmSslConnectionManager`.

Note

In previous versions of AM, this property was named `opensso.protocol.handler.pkgs`, and required a value of `com.sun.identity.protocol` if the `java.protocol.handler.pkgs` property was set by the container.

`org.forgerock.openam.audit.identity.activity.events.blacklist`

Specifies a comma-separated list of audit events that will not be logged.

The following events can be suppressed:

- `AM-ACCESS-ATTEMPT`.
- `AM-IDENTITY-CHANGE`.
- `AM-GROUP-CHANGE`.

Logging these additional events may have an impact on performance.

Default: `AM-ACCESS-ATTEMPT,AM-IDENTITY-CHANGE,AM-GROUP-CHANGE`

`org.forgerock.openam.authentication.forceAuth.enabled`

Enables or disables the ForceAuth in the *Authentication and Single Sign-On Guide* authentication parameter. If this property is set to `false` the `ForceAuth` parameter will always be `false`, regardless of what the administrator sets. If this property is `true`, the configured value of the `ForceAuth` parameter is respected.

In new installations, this property is set to `false` by default, which means that the value of `ForceAuth` is always `false`.

When you upgrade AM, this property is set to `true` by default, which means that the value of `ForceAuth` is respected.

Important

This property has no effect on authentication trees; it applies to authentication chains only. If you do not need `ForceAuth` to be enabled, it is *strongly* recommended that you set `org.forgerock.openam.authentication.forceAuth.enabled` to `false`.

Default: `false` for new installations, `true` for upgraded installations

`org.forgerock.openam.authLevel.excludeRequiredOrRequisite`

Specifies whether a session's authentication level is *always* the highest authentication level of any authentication module that passed, even if there are `requisite` or `required` modules in the authentication chain that were not executed. For more information, see "About Authentication Levels for Chains" in the *Authentication and Single Sign-On Guide*.

Default: `false`

`org.forgerock.embedded.dsadminport`

Administration port for the embedded DS server.

Default: `4444`

`org.forgerock.openam.auth.audit.nodes.enabled`

When `true`, AM generates audit log messages for each authentication node reached during authentication tree flows.

Possible values are `true` or `false`.

Default: `true`

`org.forgerock.openam.auth.audit.trees.enabled`

When `true`, AM generates audit log messages with the outcome of authentication tree flows.

Possible values are `true` or `false`.

Default: `true`

`org.forgerock.openam.auth.transactionauth.returnErrorOnAuthFailure`

Specifies whether AM returns an HTTP 200 or HTTP 401 message when the user fails to complete the required actions to perform session upgrade during transactional authorization. Possible values are:

- `false`. AM returns an HTTP 200 message with the original SSO token. For example:

```
{
        "tokenId": "AQIC5wM...TU3OQ*",
        "successUrl": "http://example.com/index.html",
        "realm": "/"
        }
```

  In this case, the user is redirected to the success URL and, when trying to access the protected resource, policy evaluation will fail since transactional authorization has failed.

- `true`. AM returns an HTTP 401 message. For example:

```
{
        "code":401,
        "reason":"Unauthorized",
        "message":"Login failure",
        "detail":{
        "failureUrl":"http://example.com/unauthorized.html"
        }
        }
```

  In this case, the user is redirected to the failure URL.

Default: `false`

`org.forgerock.openam.authentication.accountExpire.days`

Days until account expiration set after successful authentication by the account expiration post authentication plugin.

Default: `30`

`org.forgerock.openam.console.autocomplete.enabled`

Specifies whether input forms and password fields can be autocompleted. This property only affects end-user pages in the classic UI. Possible values are `true`, to enable autocomplete, and `false`, to disable it.

Default: `true`

`org.forgerock.openam.core.resource.lookup.cache.enabled`

Controls whether the results of resource file lookup should be cached.

While you are customizing the UI as described in the UI Customization Guide, set this property to `false` to allow AM immediately to pick up changes to the files as you customize them.

Reset this to the default, `true`, when using AM in production.

Default: `true`

`org.forgerock.openam.cts.rest.enabled`

Enables access to the CTS REST endpoint `/json/tokens`.

Even when access to the CTS REST endpoint is enabled, only the AM global administrator has authorization to perform operations against `/json/tokens`.

Default: `false`

After changing this property, you must restart AM or the container in which it runs for the change to take effect.

`org.forgerock.openam.encryption.key.digest`

Determines the digest algorithm used along with PBKDF2 key derivation method for AES Key Wrap encryption. Possible values are `SHA1`, `SHA256`, `SHA384`, or `SHA512`.

Set this property in AM's web container's startup script. For more information, see "Preparing AES Key Wrap Encryption" in the *Installation Guide*.

Default: `SHA1`

`org.forgerock.openam.encryption.key.iterations`

The number of iterations for the key derivation process specified in the `org.forgerock.openam.encryption.key.digest` advanced property.

Set this property in AM's web container's startup script. For more information, see "Preparing AES Key Wrap Encryption" in the *Installation Guide*.

Default:`10000`

`org.forgerock.openam.encryption.key.size`

The size of the derived key for the AES Key Wrap encryption operations.

Set this property in AM's web container's startup script. For more information, see "Preparing AES Key Wrap Encryption" in the *Installation Guide*.

Default: `128`

`org.forgerock.openam.encryption.useextractandexpand`

Enables the algorithm introduced in AM 7.1 that reduces the performance cost of AES Key Wrap encryption even when high iteration counts are used. Possible values are `true`, to enable it, and `false` to disable it.

If you configure a large iteration count when this property is set to `false`, AM startup times may see a performance impact if there are many agents in your deployment.

Set this property in AM's web container's startup script. For more information, see "Preparing AES Key Wrap Encryption" in the *Installation Guide*.

Default: `false`

`org.forgerock.openam.httpclienthandler.system.clients.connection.timeout`

Specifies the time that new client connections using ForgeRock's ClientHandler code will wait before timing out.

The value is a string specifying a number and a unit of time.

Restart AM or the container in which it runs for the change to take effect.

Default: `10 seconds`

`org.forgerock.openam.httpclienthandler.system.clients.max.connections`

Specifies the maximum number of connections allowed in the pool available for clients using ForgeRock's ClientHandler code.

Use this property only when the `org.forgerock.openam.httpclienthandler.system.clients.reuse.connections.enabled` advanced server property is enabled.

Restart AM or the container in which it runs for the change to take effect.

Default: `64`

`org.forgerock.openam.httpclienthandler.system.clients.pool.ttl`

Specifies, in milliseconds, the maximum time-to-live for pooled clients connections using ForgeRock's ClientHandler code.

Restart AM or the container in which it runs for the change to take effect.

Default: Not set

`org.forgerock.openam.httpclienthandler.system.clients.response.timeout`

Specifies the time that a client using ForgeRock's ClientHandler code will wait for a response before timing out.

The value is a string specifying a number and a unit of time.

Restart AM or the container in which it runs for the change to take effect.

Default: `10 seconds`

`org.forgerock.openam.httpclienthandler.system.clients.retry.failed.requests.enabled`

Specifies whether the ForgeRock's ClientHandler code should retry failed connections. Possible values are `true` or `false`.

Restart AM or the container in which it runs for the change to take effect.

Default: `true`

`org.forgerock.openam.httpclienthandler.system.clients.reuse.connections.enabled`

Specifies whether the ForgeRock's ClientHandler code should pool and reuse connections. Possible values are `true` or `false`.

Restart AM or the container in which it runs for the change to take effect.

Default: `true`

`org.forgerock.openam.httpclienthandler.system.nonProxyHosts`

Lists the target hosts for which requests should not be proxied. Hostnames are separated by commas.

This property supports wildcards at the start and end of any value. For example, `*.example.com` would result in a match for `customers.example.com` and `staff.example.com`, and requests would not be proxied for those target hosts.

Configure alongside the `org.forgerock.openam.httpclienthandler.system.proxy.uri`, `org.forgerock.openam.httpclienthandler.system.proxy.username`, and `org.forgerock.openam.httpclienthandler.system.proxy.password` advanced server properties.

Default: `localhost,127.*,[::1],0.0.0.0,[::0]`

`org.forgerock.openam.httpclienthandler.system.proxy.enabled`

When set to `true`, AM routes outgoing ForgeRock's ClientHandler code requests through the HTTP proxy defined on the JVM.

For more information about JVM properties, see Tip in the *Installation Guide*.

Restart AM or the container in which it runs for the change to take effect.

Default: Not set

`org.forgerock.openam.httpclienthandler.system.proxy.password`

Specifies the password of the proxy that AM will use to route outgoing ForgeRock's ClientHandler code requests.

Configure alongside the `org.forgerock.openam.httpclienthandler.system.proxy.username`, `org.forgerock.openam.httpclienthandler.system.proxy.uri`, and `org.forgerock.openam.httpclienthandler.system.nonProxyHosts` advanced server properties.

Restart AM or the container in which it runs for the change to take effect.

Default: Not set

`org.forgerock.openam.httpclienthandler.system.proxy.uri`

Specifies the URI of the proxy that AM will use to route outgoing ForgeRock's ClientHandler code requests. The URI must be in the format *`scheme://hostname:port`*. For example, `https://myproxy.example.com:443`.

If the proxy requires authentication, configure the `org.forgerock.openam.httpclienthandler.system.proxy.username` and `org.forgerock.openam.httpclienthandler.system.proxy.uri` advanced server properties as well.

This property takes precedence over the `org.forgerock.openam.httpclienthandler.system.proxy.enabled` advanced server property and its related JVM properties.

For more information, see "Configuring AM for Outbound Communication" in the *Security Guide*.

Restart AM or the container in which it runs for the change to take effect.

Default: Not set

`org.forgerock.openam.httpclienthandler.system.proxy.username`

Specifies the username of the proxy that AM will use to route outgoing ForgeRock's ClientHandler code requests.

Configure alongside the `org.forgerock.openam.httpclienthandler.system.proxy.password`, `org.forgerock.openam.httpclienthandler.system.proxy.uri`, and `org.forgerock.openam.httpclienthandler.system.nonProxyHosts` advanced server properties.

Restart AM or the container in which it runs for the change to take effect.

Default: Not set

`org.forgerock.openam.idm.attribute.names.lower.case`

Specifies whether the fields in JSON responses are always returned in lowercase. When `true`, AM converts the fields to lowercase.

Default: `false`

`org.forgerock.openam.introspect.token.query.param.allowed`

Specifies whether AM allows HTTP GET requests, *and* the use of `token` as a query parameter in POST requests, on the oauth2/introspect endpoint.

For security reasons, and in accordance with the OAuth 2.0 Token Introspection specification, AM disallows HTTP GET requests on the introspection endpoint, and requires HTTP POST requests instead. AM also disallows the use of `token` as a query parameter in a POST request on that endpoint; for example, `/oauth2/introspect?token=access-token`.

If your clients in an existing deployment need to send a GET request or `token` as a query parameter to the `oauth2/introspect` endpoint, you can change this setting to `true`. However, it is recommended that you adjust your clients to use the more secure setting.

Default: `false`

`org.forgerock.openam.ldap.default.time.limit`

Configures the client-side timeout, in milliseconds, applied to LDAP operations performed with the Netscape LDAP SDK.

Default: `0` (no time limit)

`org.forgerock.openam.ldap.dncache.expire.time`

Sets the DN cache timeout, in milliseconds, after which an entry should be removed from the cache. A value of `0` means that the DN cache will not expire, and entries will not be removed automatically.

Important

Setting this value too low can have a *severe* performance impact.

Default: `0` (no time limit)

`org.forgerock.openam.ldap.heartbeat.timeout`

Specifies the number of seconds that AM should wait for a heartbeat operation to the DS server to complete, before considering the connection unavailable.

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 `0` or to a negative number.

Default: `10`

`org.forgerock.openam.ldap.secure.protocol.version`

The protocols AM uses to connect to a secure LDAP server.

Specify a single value, for example `TLSv1.2`, for AM to use only that protocol when connecting to affected external resources. Refer to "*Securing Network Communication*" in the *Security Guide* for a list of these resources.

Specify a comma-separated list with multiple protocols for AM to use the most secure protocol supported by the external resources.

For environments using Java 11 and later, a value of `TLSv1.3,TLSv1.2` means that AM attempts to use the TLSv1.3 protocol to connect to external configuration and user data stores, but if a TLSv1.3 connection is not supported, AM uses TLSv1.2.

> **Note**
>
> Upgrading to Java 11 (versions 11.0.11, 1.8.0_291 and later) disables protocol versions TLSv1 and TLSv1.1, which are considered less secure and are now deprecated.

Default: TLSv1.3,TLSv1.2

`org.forgerock.openam.notifications.agents.enabled`

Controls whether to publish notifications for consumption by web agents and Java agents.

This property does not apply to web or Java agent versions earlier than version 5. If the deployment uses only earlier versions of web and Java agents, you can set this property to `false`.

Default: `true`

`org.forgerock.openam.openidconnect.allow.open.dynamic.registration`

Controls whether OpenID Connect clients can register dynamically without providing an access token.

If you set this to `true` in production, take care to limit or throttle dynamic client registrations.

Default: `false`

`org.forgerock.openam.radius.server.context.cache.size`

Maximum number of RADIUS client sessions that can be cached concurrently on the AM server.

Default: `5000`

`org.forgerock.openam.redirecturlvalidator.maxUrlLength`

Specifies the maximum length of redirection URLs validated by AM. The Validation Service and other AM services perform redirection URL validation.

The default value should be adequate in most cases. Increase the default value as needed if messages similar to the following appear in your debug log files with message-level debugging enabled:

```
RedirectUrlValidator.isRedirectUrlValid: The url was length 2015 which is longer than the allowed
maximum of 2000
```

Default: `2000`

`org.forgerock.openam.request.max.bytes.entity.size`

Specifies the maximum size of the body of any request made to AM. For more information, see "Limiting the Size of the Request Body" in the *Security Guide*.

The property is hot-swappable. You do not need to restart AM for the changes to take effect.

Default: 1 MB (1048576 bytes)

`org.forgerock.openam.secrets.keystore.keyid.provider`

Specifies the name of the `KeyStoreKeyIdProvider` implementation AM uses to provide key ID (`kids`) to public keys when AM is configured as an OAuth 2.0 authorization server.

For more information, see "Customizing Public Key IDs" in the *OpenID Connect 1.0 Guide*.

Default: `org.forgerock.openam.secrets.DefaultKeyStoreKeyIdProvider`.

`org.forgerock.openam.secrets.googlekms.decryptionkey`

Specifies the fully qualified resource ID of the Google Cloud KMS secret used to decrypt secrets as they are read from the filesystem, environment variables, or system properties.

This property may also specify the Google Cloud KMS secret used to decrypt the hash of the password of the `amAdmin` user, if the value of the `org.forgerock.openam.secrets.special.user.passwords.format` advanced server property is set to `GOOGLE_KMS_ENCRYPTED`.

Only one key can be specified at a time.

For more information, see "Using Google Cloud KMS Secrets to Decrypt AM Secrets" in the *Security Guide* and "Changing the amAdmin Password (Secret Stores)" in the *Security Guide*.

This property has no default.

`org.forgerock.openam.secrets.special.user.passwords.format`

Specifies the format used to store the hash of the `amAdmin` user password.

Possible values are:

- `ENCRYPTED_PLAIN`. The hash is encrypted with the AM encryption key.
- `PLAIN`. The hash is unencrypted. The password **must** be randomly generated and high entropy.
- `GOOGLE_KMS_ENCRYPTED`. The hash is encrypted with the Google Cloud KMS secret specified in the `org.forgerock.openam.secrets.googlekms.decryptionkey` advanced server property.

For more information, see "Changing the amAdmin Password (Secret Stores)" in the *Security Guide*.

Default: `ENCRYPTED_PLAIN`

`org.forgerock.openam.session.stateless.encryption.method`

Sets the encryption method for client-based sessions. Possible values are:

- **A128CBC-HS256**. AES 128-bit in CBC mode using HMAC-SHA-256-128 hash (HS256 truncated to 128 bits)
- **A192CBC-HS384**. AES 192-bit in CBC mode using HMAC-SHA-384-192 hash (HS384 truncated to 192 bits)
- **A256CBC-HS512**. AES 256-bit in CBC mode using HMAC-SHA-512-256 hash (HS512 truncated to 256 bits)
- **A128GCM**. AES 128-bit in GCM mode
- **A192GCM**. AES 192-bit in GCM mode
- **A256GCM**. AES 256-bit in GCM mode

Default: `A128CBC-HS256`

`org.forgerock.openam.session.stateless.rsa.padding`

Sets the padding mode for RSA encryption of client-based sessions. Possible values are:

- **RSA1_5**. RSA with PKCS#1 v1.5 padding.
- **RSA-OAEP**. RSA with OAEP and SHA-1.
- **RSA-OAEP-256**. RSA with OAEP padding and SHA-256.

Default: `RSA-OAEP-256`

`org.forgerock.openam.session.stateless.signing.allownone`

Specifies whether signing client-based sessions is enabled. When `true`, AM allows selecting `NONE` as the signing algorithm for client-based sessions under Configure > Global Services > Session > Client-based Sessions.

`org.forgerock.openam.smtp.system.connect.timeout`

Specifies the amount of time, in milliseconds, that AM waits before considering that an outbound SMTP connection is unavailable.

Default: 10000

`org.forgerock.openam.smtp.system.socket.read.timeout`

Specifies the amount of time, in milliseconds, that AM waits for an SMTP read request to receive an acknowledgement before returning an error.

Default: 10000

`org.forgerock.openam.smtp.system.socket.write.timeout`

Specifies the amount of time, in milliseconds, that AM waits for an SMTP write request to receive an acknowledgement before returning an error.

Default: 10000

`org.forgerock.openam.slf4j.enableTraceInMessage`

Controls whether trace-level logging messages are generated when message-level debug logging is enabled in AM.

Certain components that run in AM's JVM—for example, embedded DS configuration stores—write a large volume of trace-level debug records that are not required for troubleshooting in many cases. With this option set to `false`, trace-level debug records are not written for these components.

If you set this to `true` in production, take care to monitor the amount of disk space occupied by the AM debug logs.

Default: `false`

`org.forgerock.openam.sso.providers.list`

Specifies an ordered list of SSO providers. AM chooses the first applicable provider depending on the context for the requested SSO operation.

Default: `org.forgerock.openidconnect.ssoprovider.OpenIdConnectSSOProvider, org.forgerock.openam.sso.providers.stateless.StatelessSSOProvider`

`org.forgerock.openam.trees.consumedstatedata.cache.size`

Specifies the maximum number of trees in a realm for which to cache the results of "state" scans.

AM recursively scans the nodes and paths in authentication trees to determine the state data that each node consumes. Caching this information for a number of trees in each realm means AM does not have to make multiple calls to get the tree's structure.

If you have many complex authentication trees and a large number of realms, increasing this value may reduce the impact on performance of the consumed state scans.

Default: `15`

`org.forgerock.openam.xui.user.session.validation.enabled`

Changes the UI's behavior when a user session expires. Possible values are `false`, where the user notices that their session has expired when trying to interact with the UI and they are redirected to the login screen, or `true`, where AM redirects the user to a page with the session expired message when their session expires. This prevents the display of possible sensitive information on the screen after a session expires.

This setting does not apply to those users that are global or realm administrators, for example, `amAdmin`.

Default: `true`

`org.forgerock.openidconnect.ssoprovider.maxcachesize`

Maximum size in entries of the `OpenIdConnectSSOProvider` provider's cache. This cache is used to map OIDC tokens to SSO tokens for quick lookup.

Default: `5000`

`org.forgerock.policy.subject.evaluation.cache.size`

Maintains a record of subject IDs matched or not matched in a given session. The cache is keyed on the token ID and the session is cleared when destroyed.

Default: `10000`

`org.forgerock.security.oauth2.enforce.sub.claim.uniqueness`

Specifies the format of the subject (`sub`) claim of an OAuth 2.0 access token, logout token in the *OpenID Connect 1.0 Guide*, and OpenID Connect ID token. Possible values are:

- `false`.

  The value of the `sub` claim is the username of the identity, or the name or the client that is the subject of the token.

  For example, `demo`, or `myOauth2Client`.

- `true`.

  The subject claim is in the format `(type!subject)`, where:

  - `subject` is the identifier of the user/identity, or the name of the OAuth 2.0/OpenID Connect client that is the subject of the token.
  - `type` can be one of the following:
    - `age`. Specifies that the *subject* is an OAuth 2.0/OpenID Connect-related user-agent or client. For example, an OAuth 2.0 client, a Remote Consent Service agent, and a Web and Java Agent internal client.

- `usr`. Specifies that the *subject* is a user/identity.

For example, `(usr!demo)`, or `(age!myOAuth2Client)`.

Tokens using the old `sub` format will still be accepted after the property is enabled.

Before enabling this property, ensure that your clients can use the new `sub` claim format, or a combination of the `sub` and the `subname` claims.

+ *About the subname Claim*

The value of the `subname` claim matches the value of the `sub` claim as it was returned in versions of AM earlier than 7.1, or as returned when the `org.forgerock.security.oauth2.enforce.sub.claim.uniqueness` advanced server property is disabled.

An example of the value of the `subname` claim is `demo`, or `myOauth2Client`.

This claim was introduced in AM 7.1, and is added by default to access and logout tokens. It is also available to ID tokens, but not included in the `OIDC Claims Script`. Therefore, AM does not add it to ID tokens by default.

Default: `true` for new installations, `false` for upgrades

`org.forgerock.services.cts.queue.readiness.threshold`

The threshold, in percentage of CTS queue usage, when considering if an AM instance is ready to process further requests.

The `/json/health/ready` endpoint returns an HTTP 503 error if the following are *both true*:

1. The CTS queue is more full than the value configured in this property.
2. The CTS data store is available.

A queue that is filling up even though there is a CTS store available to process it could indicate that the health of the AM instance is below expectations. That is why the endpoint returns HTTP 503.

Specify an integer threshold value, representing a percentage of CTS queue size. The value must be between `1` and `100`, inclusive. Specifying a value outside this range causes AM to use the default value.

Default: `90` (percent)

For more information, see "*Monitoring Instances*" in the *Maintenance Guide*.

`org.forgerock.services.cts.reaper.cache.pollFrequencyMilliseconds`

How often to poll the reaper cache for tokens that have expired, and delete them.

By default, an AM instance will review its cache for tokens eligible for deletion every 100 milliseconds.

Default: `100` (milliseconds)

For more information, see "Reaper Cache Size" in the *Core Token Service Guide (CTS)*.

`org.forgerock.services.cts.reaper.cache.size`

The number of records an AM instance will store in its CTS reaper cache.

Default: `500000`

For more information, see "Reaper Cache Size" in the *Core Token Service Guide (CTS)*.

`org.forgerock.services.cts.reaper.search.gracePeriodMilliseconds`

Specifies a grace period used when searching for expired tokens. Any tokens that expired more than the specified duration ago are returned.

Default: `300000` (milliseconds)

For more information, see "Reaper Cache Size" in the *Core Token Service Guide (CTS)*.

`org.forgerock.services.cts.reaper.search.pollFrequencyMilliseconds`

How often to perform a search for expired tokens in the CTS persistence store.

Default: `5000` (milliseconds)

For more information, see "Reaper Cache Size" in the *Core Token Service Guide (CTS)*.

`org.forgerock.services.cts.reaper.search.tokenLimit`

The maximum number of expired tokens to return to the AM reaper when searching the CTS store.

Default: `5000`

For more information, see "Reaper Cache Size" in the *Core Token Service Guide (CTS)*.

`org.forgerock.services.cts.store.ttlsupport.enabled`

Specifies whether AM support for the DS entry expiration and deletion feature is enabled. Enabling this setting causes AM to clone the value of the `coreTokenExpirationDate` attribute to the `coreTokenTtlDate` attribute during token creation, which allows DS to index tokens using the `coreTokenTtlDate` attribute for the entry expiration and deletion feature.

This property does not clone the values of tokens that were created before the setting was enabled.

Set this property to `true` in conjunction with the `org.forgerock.services.cts.store.ttlsupport.exclusionlist` advanced server property when you need to configure the AM reaper to manage the expiration time for a subset of the tokens in the CTS store only.

For more information, see "*Configuring the CTS Reaper*" in the *Core Token Service Guide (CTS)*.

Default: `false`

`org.forgerock.services.cts.store.reaper.enabled`

Specifies whether the AM reaper is enabled.

> **Important**
>
> Do not disable the AM reaper unless you have a system in place to clean up expired tokens, such as the DS entry expiration and deletion feature.

Set this property to `true` in the following scenarios:

- When the AM reaper must manage the expiration times for all the tokens in the CTS store.
- When the AM reaper must manage the expiration time for a subset of the tokens in the CTS store.

For more information, see "*Configuring the CTS Reaper*" in the *Core Token Service Guide (CTS)*.

Default: `true`

`org.forgerock.services.cts.store.ttlsupport.exclusionlist`

When the `org.forgerock.services.cts.store.ttlsupport.enabled` advanced server property is set to `true`, this property specifies a list of token types which will not have their `coreTokenExpirationDate` data cloned. For example, `SESSION`.

The AM reaper will delete the excluded tokens when they expire.

> **Tip**
>
> You can see the token types in use in your environment inside the CTS token store.

For more information, see "*Configuring the CTS Reaper*" in the *Core Token Service Guide (CTS)*.

Default: Not set

`org.forgerock.services.datalayer.connection.timeout`

Timeout in seconds for LDAP connections to the configuration data store.

Default: `10` (seconds)

For suggested settings, see "Tuning CTS Store LDAP Connections" in the *Maintenance Guide*.

`org.forgerock.services.datalayer.connection.timeout.cts.async`

Timeout in seconds for LDAP connections used for most CTS operations.

Default: `10` (seconds)

For suggested settings, see "Tuning CTS Store LDAP Connections" in the *Maintenance Guide*.

`org.forgerock.services.datalayer.connection.timeout.cts.reaper`

Timeout in seconds for the LDAP connection used for CTS token cleanup.

Default: None (do not time out)

For suggested settings, see "Tuning CTS Store LDAP Connections" in the *Maintenance Guide*.

org.forgerock.openam.ldap.keepalive.search.base

Defines the search base for:

- The heartbeat request that checks connections to the LDAP server are alive and prevents idle timeouts (keepalive).
- The load balancer availability check.

The keepalive and availability checks are only enabled if the heartbeat interval and timeout are set to a value greater than 0.

The LDAP server connection pool will be marked as unavailable if the search fails with an error, returns no entries, or if more than one entry is returned.

If the search results in an error, AM fails to start up with an exception such as `org.forgerock.opendj.ldap.ConnectionException: Connect Error: No operational connection factories available`.

ssoadm attribute: `openam-idrepo-ldapv3-keepalive-searchbase`

Default: `[Empty]`

org.forgerock.openam.ldap.keepalive.search.filter

Defines the search filter for:

- The heartbeat request that checks connections to the LDAP server are alive and prevents idle timeouts (keepalive).
- The load balancer availability check.

You can also use the absolute True and False filter (`&`).

The LDAP server connection pool will be marked as unavailable if the search fails with an error, returns no entries, or if more than one entry is returned.

If the search results in an error, AM fails to start up with an exception such as `org.forgerock.opendj.ldap.ConnectionException: Connect Error: No operational connection factories available`.

ssoadm attribute: `openam-idrepo-ldapv3-keepalive-searchfilter`

Default: `(objectClass=*)`

`securidHelper.ports`

Port on which SecurID daemon listens.

Default: 58943

Configuring Sites

Sites involve multiple AM servers working together to provide services. You can use sites with load balancers and session high availability to configure pools of servers capable of responding to client requests in highly available fashion.

Name

Sets the name of the site.

Primary URL

Sets the primary entry point to the site, such as the URL, to the load balancer for the site configuration.

Secondary URLs

Sets alternate entry points to the site.

Chapter 4

Global Services Configuration

Under Configure > Global Services, you can set defaults for a range of AM services.

Audit Logging

amster service name: `audit`

Global Attributes

The following settings appear on the **Global Attributes** tab:

Audit logging

Enable audit logging in AM.

Default value: `true`

amster attribute: `auditEnabled`

Field whitelist filters

AM 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.

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 `access`, `activity`, `authentication`, or `config`.

For example, to record the values of the `Accept-Language` HTTP header in *access* events, the pointer is `/access/http/request/headers/accept-language`.

amster attribute: `whitelistFieldFilters`

Field blacklist filters

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.

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 `access`, `activity`, `authentication`, or `config`.

For example, you might want to filter out surnames by hiding the `sn` field from *activity* events. To do so, add the following pointers to the Field blacklist filters list:

- `/activity/before/sn`
- `/activity/after/sn`

amster attribute: `blacklistFieldFilters`

Realm Defaults

The following settings appear on the **Realm Defaults** tab:

Audit logging

Enable audit logging in AM.

Default value: `true`

amster attribute: `auditEnabled`

Field whitelist filters

AM 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.

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 `access`, `activity`, `authentication`, or `config`.

For example, to record the values of the `Accept-Language` HTTP header in *access* events, the pointer is `/access/http/request/headers/accept-language`.

amster attribute: `whitelistFieldFilters`

Field blacklist filters

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.

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 `access`, `activity`, `authentication`, or `config`.

For example, you might want to filter out surnames by hiding the `sn` field from *activity* events. To do so, add the following pointers to the Field blacklist filters list:

- `/activity/before/sn`
- `/activity/after/sn`

amster attribute: `blacklistFieldFilters`

Secondary Configurations

This service has the following Secondary Configurations.

JMS

A configured secondary instance of the JMS type has the following tabs:

General Handler Configuration

The General Handler Configuration tab contains the following secondary configuration properties:

Enabled

Enables or disables an audit event handler.

Default value: `true`

amster attribute: `enabled`

Topics

List of topics handled by an audit event handler.

Default value:

```
access
activity
config
authentication
```

amster attribute: `topics`

Audit Event Handler Factory

The Audit Event Handler Factory tab contains the following secondary configuration properties:

Factory Class Name

The fully qualified class name of the factory responsible for creating the Audit Event Handler. The class must implement `org.forgerock.openam.audit.AuditEventHandlerFactory`.

Default value: `org.forgerock.openam.audit.events.handlers.JmsAuditEventHandlerFactory`

amster attribute: `handlerFactory`

JMS Configuration

The JMS Configuration tab contains the following secondary configuration properties:

Delivery Mode

Specifies whether JMS messages used to transmit audit events use persistent or non-persistent delivery.

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.

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.

Default value: `NON_PERSISTENT`

amster attribute: `deliveryMode`

Session Mode

Specifies the JMS session acknowledgement mode: `AUTO`, `CLIENT`, or `DUPS_OK`.

- Auto mode guarantees once-only delivery of JMS messages used to transmit audit events.
- Duplicates OK mode ensures that messages are delivered at least once.
- Client mode does not ensure delivery.

Use the default setting unless your JMS broker implementation requires otherwise. See your broker documentation for more information.

Default value: `AUTO`

amster attribute: `sessionMode`

JNDI Context Properties

Specifies JNDI properties that AM uses to connect to the JMS message broker to which AM will publish audit events.

AM acts as a JMS client, using a JMS connection factory to connect to your JMS message broker. In order for AM 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.

The default properties are example properties for connecting to Apache ActiveMQ.

Default value:

```
{
```

```
    "java.naming.factory.initial": "org.apache.activemq.jndi.ActiveMQInitialContextFactory",
    "topic.audit": "audit",
    "java.naming.provider.url": "tcp://localhost:61616"
}
```

amster attribute: `jndiContextProperties`

JMS Topic Name

JNDI lookup name for the JMS topic

Default value: `audit`

amster attribute: `jndiTopicName`

JMS Connection Factory Name

Specifies the JNDI lookup name for the connection factory exposed by your JMS message broker. AM performs a JNDI lookup on this name to locate your broker's connection factory.

See the documentation for your JMS message broker for the required value.

The default is the connection factory name for Apache ActiveMQ.

Default value: `ConnectionFactory`

amster attribute: `jndiConnectionFactoryName`

Batch Events

The Batch Events tab contains the following secondary configuration properties:

Capacity

Maximum event count in the batch queue; additional events are dropped.

Default value: `1000`

amster attribute: `batchCapacity`

Max Batched

Maximum number of events per batch.

Default value: `100`

amster attribute: `maxBatchedEvents`

Writing Interval

The interval (in seconds) for reading events from the buffer to transmit via jms.

Default value: `10`

amster attribute: `pollTimeoutSec`

JSONStdout

A configured secondary instance of the JSONStdout type has the following tabs:

General Handler Configuration

The General Handler Configuration tab contains the following secondary configuration properties:

Enabled

Enables or disables an audit event handler.

Default value: `true`

amster attribute: `enabled`

Topics

List of topics handled by an audit event handler.

Default value:

```
access
activity
config
authentication
```

amster attribute: `topics`

Audit Event Handler Factory

The Audit Event Handler Factory tab contains the following secondary configuration properties:

Factory Class Name

The fully qualified class name of the factory responsible for creating the Audit Event Handler. The class must implement `org.forgerock.openam.audit.AuditEventHandlerFactory`.

Default value: `org.forgerock.openam.audit.events.handlers.JsonStdoutAuditEventHandlerFactory`

amster attribute: `handlerFactory`

JSON Configuration

The JSON Configuration tab contains the following secondary configuration properties:

ElasticSearch JSON Format Compatible

JSON format should be transformed to be compatible with ElasticSearch format restrictions.

Default value: `false`

amster attribute: `elasticsearchCompatible`

Elasticsearch

A configured secondary instance of the Elasticsearch type has the following tabs:

General Handler Configuration

The General Handler Configuration tab contains the following secondary configuration properties:

Enabled

Enables or disables an audit event handler.

Default value: `true`

amster attribute: `enabled`

Topics

List of topics handled by an audit event handler.

Default value:

```
access
activity
config
authentication
```

amster attribute: `topics`

Audit Event Handler Factory

The Audit Event Handler Factory tab contains the following secondary configuration properties:

Factory Class Name

The fully qualified class name of the factory responsible for creating the Audit Event Handler. The class must implement `org.forgerock.openam.audit.AuditEventHandlerFactory`.

Default value: `org.forgerock.openam.audit.events.handlers.ElasticsearchAuditEventHandlerFactory`

amster attribute: `handlerFactory`

Elasticsearch Configuration

The Elasticsearch Configuration tab contains the following secondary configuration properties:

Server Hostname

Host name or IP address of the Elasticsearch server.

amster attribute: `host`

Server Port

Specifies the port number used to access Elasticsearch's REST API.

amster attribute: `port`

SSL Enabled

Specifies whether SSL is configured on the Elasticsearch server.

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 AM before attempting to log audit events to Elasticsearch.

Default value: `false`

amster attribute: `sslEnabled`

Elasticsearch Index

Specifies the name of the Elasticsearch index to be used for AM audit logging.

amster attribute: `index`

Authentication

The Authentication tab contains the following secondary configuration properties:

Username

Specifies the username to access the Elasticsearch server.

Required if Elasticsearch Shield authentication is configured.

amster attribute: `username`

Password

Specifies the password to access the Elasticsearch server.

Required if Elasticsearch Shield authentication is configured.

amster attribute: `password`

Buffering

The Buffering tab contains the following secondary configuration properties:

Buffering Enabled

Default value: `true`

amster attribute: `bufferingEnabled`

Batch Size

Maximum number of events that can be buffered (default: 10000)

Default value: `500`

amster attribute: `batchSize`

Queue Capacity

Maximum number of audit logs in the batch queue. Additional audit events are dropped.

Default value: `10000`

amster attribute: `maxEvents`

Write interval (in milliseconds)

Specifies the interval in milliseconds at which buffered events are written to Elasticsearch.

Default value: `250`

amster attribute: `writeInterval`

Syslog

A configured secondary instance of the Syslog type has the following tabs:

General Handler Configuration

The General Handler Configuration tab contains the following secondary configuration properties:

Enabled

Enables or disables an audit event handler.

Default value: `true`

amster attribute: `enabled`

Topics

List of topics handled by an audit event handler.

Default value:

```
access
activity
config
authentication
```

amster attribute: `topics`

Audit Event Handler Factory

The Audit Event Handler Factory tab contains the following secondary configuration properties:

Factory Class Name

The fully qualified class name of the factory responsible for creating the Audit Event Handler. The class must implement `org.forgerock.openam.audit.AuditEventHandlerFactory`.

Default value: `org.forgerock.openam.audit.events.handlers.SyslogAuditEventHandlerFactory`

amster attribute: `handlerFactory`

Syslog Configuration

The Syslog Configuration tab contains the following secondary configuration properties:

Server hostname

Host name or IP address of receiving syslog server.

amster attribute: `host`

Server port

Port number of receiving syslog server.

amster attribute: `port`

Transport Protocol

Default value: `TCP`

amster attribute: `transportProtocol`

Connection timeout

Timeout for connecting to syslog server, in seconds.

amster attribute: `connectTimeout`

Facility

Syslog facility value to apply to all events.

Default value: `USER`

amster attribute: `facility`

Buffering

The Buffering tab contains the following secondary configuration properties:

Buffering Enabled

Enables or disables audit event buffering.

Default value: `true`

amster attribute: `bufferingEnabled`

Buffer Size

Maximum number of events that can be buffered (default/minimum: 5000)

Default value: `5000`

amster attribute: `bufferingMaxSize`

CSV

A configured secondary instance of the CSV type has the following tabs:

General Handler Configuration

The General Handler Configuration tab contains the following secondary configuration properties:

Enabled

Enables or disables an audit event handler.

Default value: `true`

amster attribute: `enabled`

Topics

List of topics handled by an audit event handler.

Default value:

```
access
activity
config
authentication
```

amster attribute: `topics`

Audit Event Handler Factory

The Audit Event Handler Factory tab contains the following secondary configuration properties:

Factory Class Name

The fully qualified class name of the factory responsible for creating the Audit Event Handler. The class must implement `org.forgerock.openam.audit.AuditEventHandlerFactory`.

Default value: `org.forgerock.openam.audit.events.handlers.CsvAuditEventHandlerFactory`

amster attribute: `handlerFactory`

CSV Configuration

The CSV Configuration tab contains the following secondary configuration properties:

Log Directory

Directory in which to store audit log CSV files.

Default value: `%BASE_DIR%/var/audit/`

amster attribute: `location`

File Rotation

The File Rotation tab contains the following secondary configuration properties:

Rotation Enabled

Enables and disables audit file rotation.

Default value: `true`

amster attribute: `rotationEnabled`

Maximum File Size

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.

Default value: `100000000`

amster attribute: `rotationMaxFileSize`

File Rotation Prefix

Prefix to prepend to audit files when rotating audit files.

amster attribute: `rotationFilePrefix`

File Rotation Suffix

Suffix to append to audit files when they are rotated. Suffix should be a timestamp.

Default value: `-yyyy.MM.dd-HH.mm.ss`

amster attribute: `rotationFileSuffix`

Rotation Interval

Interval to trigger audit file rotations, in seconds. A negative or zero value disables this feature.

Default value: `-1`

amster attribute: `rotationInterval`

Rotation Times

Durations after midnight to trigger file rotation, in seconds.

amster attribute: `rotationTimes`

File Retention

The File Retention tab contains the following secondary configuration properties:

Maximum Number of Historical Files

Maximum number of backup audit files allowed. A value of `-1` disables pruning of old history files.

Default value: `1`

amster attribute: `retentionMaxNumberOfHistoryFiles`

Maximum Disk Space

The maximum amount of disk space the audit files can occupy, in bytes. A negative or zero value indicates this policy is disabled.

Default value: `-1`

amster attribute: `retentionMaxDiskSpaceToUse`

Minimum Free Space Required

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.

Default value: `-1`

amster attribute: `retentionMinFreeSpaceRequired`

Buffering

The Buffering tab contains the following secondary configuration properties:

Buffering Enabled

Enables or disables buffering.

Default value: `true`

amster attribute: `bufferingEnabled`

Flush Each Event Immediately

Performance may be improved by writing all buffered events before flushing.

Default value: `false`

amster attribute: `bufferingAutoFlush`

Tamper Evident Configuration

The Tamper Evident Configuration tab contains the following secondary configuration properties:

Is Enabled

Enables the CSV tamper evident feature.

Default value: `false`

amster attribute: `securityEnabled`

Certificate Store Location

Path to Java keystore.

Default value: `%BASE_DIR%/var/audit/Logger.jks`

amster attribute: `securityFilename`

Certificate Store Password

Password for Java keystore.

amster attribute: `securityPassword`

Signature Interval

Signature generation interval, in seconds.

Default value: `900`

amster attribute: `securitySignatureInterval`

JDBC

A configured secondary instance of the JDBC type has the following tabs:

General Handler Configuration

The General Handler Configuration tab contains the following secondary configuration properties:

Enabled

Enables or disables an audit event handler.

Default value: `true`

amster attribute: `enabled`

Topics

List of topics handled by an audit event handler.

Default value:

```
access
activity
config
authentication
```

amster attribute: `topics`

Audit Event Handler Factory

The Audit Event Handler Factory tab contains the following secondary configuration properties:

Factory Class Name

The fully qualified class name of the factory responsible for creating the Audit Event Handler. The class must implement `org.forgerock.openam.audit.AuditEventHandlerFactory`.

Default value: `org.forgerock.openam.audit.events.handlers.JdbcAuditEventHandlerFactory`

amster attribute: `handlerFactory`

Database Configuration

The Database Configuration tab contains the following secondary configuration properties:

Database Type

Select the database to use for logging audit events.

Identifies the database in use, for example MySQL, Oracle, or SQL.

Default value: `oracle`

amster attribute: `databaseType`

JDBC Database URL

URL of the JDBC database.

amster attribute: `jdbcUrl`

JDBC Driver

Fully qualified JDBC driver class name.

amster attribute: `driverClassName`

Database Username

Specifies the username to access the database server.

amster attribute: `username`

Database Password

Specifies the password to access the database server.

amster attribute: `password`

Connection Timeout (seconds)

Specifies the maximum wait time before failing the connection, in seconds.

Default value: `30`

amster attribute: `connectionTimeout`

Maximum Connection Idle Timeout (seconds)

Specifies the maximum idle time before the connection is closed, in seconds.

Default value: `600`

amster attribute: `idleTimeout`

Maximum Connection Time (seconds)

Specifies the maximum time a JDBC connection can be open, in seconds.

Default value: `1800`

amster attribute: `maxLifetime`

Minimum Idle Connections

Specifies the minimum number of idle connections in the connection pool.

Default value: `10`

amster attribute: `minIdle`

Maximum Connections

Specifies the maximum number of connections in the connection pool.

Default value: `10`

amster attribute: `maxPoolSize`

Buffering

The Buffering tab contains the following secondary configuration properties:

Buffering Enabled

Enables or disables audit event buffering.

Default value: `true`

amster attribute: `bufferingEnabled`

Buffer Size (number of events)

Size of the queue where events are buffered before they are written to the database.

This queue has to be big enough to store all incoming events that have not yet been written to the database.

If the queue reaches capacity, the process will block until a write occurs.

Default value: `100000`

amster attribute: `bufferingMaxSize`

Write Interval

Specifies the interval (seconds) at which buffered events are written to the database.

Default value: `5`

amster attribute: `bufferingWriteInterval`

Writer Threads

Specifies the number of threads used to write the buffered events.

Default value: `1`

amster attribute: `bufferingWriterThreads`

Max Batched Events

Specifies the maximum number of batched statements the database can support per connection.

Default value: `100`

amster attribute: `bufferingMaxBatchedEvents`

JSON

A configured secondary instance of the JSON type has the following tabs:

General Handler Configuration

The General Handler Configuration tab contains the following secondary configuration properties:

Enabled

Enables or disables an audit event handler.

Default value: `true`

amster attribute: `enabled`

Topics

List of topics handled by an audit event handler.

Default value:

```
access
activity
config
authentication
```

amster attribute: `topics`

Audit Event Handler Factory

The Audit Event Handler Factory tab contains the following secondary configuration properties:

Factory Class Name

The fully qualified class name of the factory responsible for creating the Audit Event Handler. The class must implement `org.forgerock.openam.audit.AuditEventHandlerFactory`.

Default value: `org.forgerock.openam.audit.events.handlers.JsonAuditEventHandlerFactory`

amster attribute: `handlerFactory`

JSON Configuration

The JSON Configuration tab contains the following secondary configuration properties:

Log Directory

Directory in which to store audit log JSON files.

Default value: `%BASE_DIR%/var/audit/`

amster attribute: `location`

ElasticSearch JSON Format Compatible

JSON format should be transformed to be compatible with ElasticSearch format restrictions.

Default value: `false`

amster attribute: `elasticsearchCompatible`

File Rotation Retention Check Interval

Interval to check time-based file rotation policies, in seconds.

Default value: `5`

amster attribute: `rotationRetentionCheckInterval`

File Rotation

The File Rotation tab contains the following secondary configuration properties:

Rotation Enabled

Enables and disables audit file rotation.

Default value: `true`

amster attribute: `rotationEnabled`

Maximum File Size

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.

Default value: `100000000`

amster attribute: `rotationMaxFileSize`

File Rotation Prefix

Prefix to prepend to audit files when rotating audit files.

amster attribute: `rotationFilePrefix`

File Rotation Suffix

Suffix to append to audit files when they are rotated. Suffix should be a timestamp.

Default value: `-yyyy.MM.dd-HH.mm.ss`

amster attribute: `rotationFileSuffix`

Rotation Interval

Interval to trigger audit file rotations, in seconds. A negative or zero value disables this feature.

Default value: `-1`

amster attribute: `rotationInterval`

Rotation Times

Durations after midnight to trigger file rotation, in seconds.

amster attribute: `rotationTimes`

File Retention

The File Retention tab contains the following secondary configuration properties:

Maximum Number of Historical Files

Maximum number of backup audit files allowed. A value of `-1` disables pruning of old history files.

Default value: `1`

amster attribute: `retentionMaxNumberOfHistoryFiles`

Maximum Disk Space

The maximum amount of disk space the audit files can occupy, in bytes. A negative or zero value indicates this policy is disabled.

Default value: `-1`

amster attribute: `retentionMaxDiskSpaceToUse`

Minimum Free Space Required

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.

Default value: `-1`

amster attribute: `retentionMinFreeSpaceRequired`

Buffering

The Buffering tab contains the following secondary configuration properties:

Batch Size

Maximum number of events that can be buffered (default/minimum: 100000)

Default value: `100000`

amster attribute: `bufferingMaxSize`

Write interval

Interval at which buffered events are written to a file, in milliseconds.

Default value: `5`

amster attribute: `bufferingWriteInterval`

Splunk

A configured secondary instance of the Splunk type has the following tabs:

General Handler Configuration

The General Handler Configuration tab contains the following secondary configuration properties:

Enabled

Enables or disables an audit event handler.

Default value: `true`

amster attribute: `enabled`

Topics

List of topics handled by an audit event handler.

Default value:

```
access
activity
config
authentication
```

amster attribute: `topics`

Audit Event Handler Factory

The Audit Event Handler Factory tab contains the following secondary configuration properties:

Factory Class Name

The fully qualified class name of the factory responsible for creating the Audit Event Handler. The class must implement `org.forgerock.openam.audit.AuditEventHandlerFactory`.

Default value: `org.forgerock.openam.audit.events.handlers.SplunkAuditEventHandlerFactory`

amster attribute: `handlerFactory`

Splunk Configuration

The Splunk Configuration tab contains the following secondary configuration properties:

Authorization Token

Authorization token used to connect to Splunk HTTP Event Collector endpoint.

amster attribute: `authzToken`

Server Hostname

Host name or IP address of Splunk server.

amster attribute: `host`

Server Port

Port number of Splunk server.

amster attribute: `port`

SSL Enabled

Use HTTPS protocol for communication with Splunk.

Default value: `false`

amster attribute: `sslEnabled`

Buffering

The Buffering tab contains the following secondary configuration properties:

Batch Size

Maximum number of events that can be buffered (default: 10000).

Default value: `500`

amster attribute: `batchSize`

Queue Capacity

Maximum number of audit evens in the batch queue; additional events are dropped.

Default value: `10000`

amster attribute: `maxEvents`

Write interval (in milliseconds)

Interval at which buffered events are written to Splunk.

Default value: `250`

amster attribute: `writeInterval`

Base URL Source

amster service name: `BaseUrlSource`

Realm Defaults

The following settings appear on the **Realm Defaults** tab:

Base URL Source

Specifies how the base URL is generated. Choose from the following:

- **Extension class** (Value: `EXTENSION_CLASS`)

  The extension class returns a base URL from a provided HttpServletRequest. In the Extension class name field, enter `org.forgerock.openam.services.baseurl.BaseURLProvider`.

- **Fixed value** (Value: `FIXED_VALUE`)

  The base URL is retrieved from the value specified in the Fixed value base URL field.

- **Forwarded header** (Value: `FORWARDED_HEADER`)

  The base URL is retrieved from a forwarded header field in the HTTP request. The Forwarded HTTP header field is standardized and specified in RFC7239.

- **Host/protocol from incoming request** (Value: `REQUEST_VALUES`)

  The hostname, server name, and port are retrieved from the incoming HTTP request.

- **X-Forwarded-* headers** (Value: `X_FORWARDED_HEADERS`)

  The base URL is retrieved from non-standard header fields, such as `X-Forwarded-For`, `X-Forwarded-By`, `X-Forwarded-Proto`, `X-Forwarded-Host`, and `X-Forwarded-Port`.

  If the `X-Forwarded-Proto` header is not provided, the server uses a fallback scheme, based on the URI of the request.

  If multiple `X-Forwarded-Host` headers are specified, the outermost proxy host is used.

Default value: `REQUEST_VALUES`

amster attribute: `source`

Fixed value base URL

If Fixed value is selected as the Base URL source, enter the base URL in the Fixed value base URL field.

amster attribute: `fixedValue`

Extension class name

If Extension class is selected as the Base URL source, enter `org.forgerock.openam.services.baseurl.BaseURLProvider` in the Extension class name field.

amster attribute: `extensionClassName`

Context path

Specifies the context path for the base URL.

If provided, the base URL includes the deployment context path appended to the calculated URL.

For example, `/openam`.

Default value: `/openam`

amster attribute: `contextPath`

Common Federation Configuration

amster service name: `CommonFederationConfiguration`

General Configuration

The following settings appear on the **General Configuration** tab:

Maximum allowed content length

The maximum content length allowed in federation communications, in bytes.

Default value: `20480`

amster attribute: `maxContentLength`

Check presence of certificates

Enable checking of certificates against local copy

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.

The possible values for this property are:

- `off`. Disabled
- `on`. Enabled

Default value: `on`

amster attribute: `certificateChecking`

SAML Error Page URL

AM redirects users here when an error occurs in the SAML2 engine.

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.

Default value: `/saml2/jsp/saml2error.jsp`

amster attribute: `samlErrorPageUrl`

SAML Error Page HTTP Binding

The possible values are HTTP-Redirect or HTTP-POST.

Default value: `HTTP-POST`

amster attribute: `samlErrorPageHttpBinding`

Implementation Classes

The following settings appear on the **Implementation Classes** tab:

Datastore SPI implementation class

The Federation system uses this class to get/set user profile attributes.

The default implementation uses the Identity repository APIs to access user profile attributes. A custom implementation must implement the `com.sun.identity.plugin.datastore.DataStoreProvider` interface.

Default value: `com.sun.identity.plugin.datastore.impl.IdRepoDataStoreProvider`

amster attribute: `datastoreClass`

Root URL provider SPI implementation class

The Federation system uses this class to get the root URL of the AM deployment.

The default implementation uses the Root URL APIs to access the AM instance root url. A custom implementation must implement the `org.forgerock.openam.federation.plugin.rooturl.RootUrlProvider` interface.

Default value: `org.forgerock.openam.federation.plugin.rooturl.impl.FmRootUrlProvider`

amster attribute: `rootUrlProviderClass`

ConfigurationInstance SPI implementation class

The Federation system uses this class to fetch service configuration.

The default implementation uses the SMS APIs to access service configuration. A custom implementation must implement the `com.sun.identity.plugin.configuration.ConfigurationInstance` interface.

Default value: `com.sun.identity.plugin.configuration.impl.ConfigurationInstanceImpl`

amster attribute: `configurationClass`

Logger SPI implementation class

The Federation system uses this class to record log entries.

The default implementation uses the Logging APIs to record log entries. A custom implementation must implement the `com.sun.identity.plugin.log.Logger` interface.

Default value: `com.sun.identity.plugin.log.impl.LogProvider`

amster attribute: `loggerClass`

SessionProvider SPI implementation class

The Federation system uses this class to interface with the session service.

The default implementation uses the standard authentication and SSO APIs to access the session service. A custom implementation must implement the `com.sun.identity.plugin.session.SessionProvider` interface.

Default value: `com.sun.identity.plugin.session.impl.FMSessionProvider`

amster attribute: `sessionProviderClass`

PasswordDecoder SPI implementation class

The Federation system uses this class to decode password encoded by AM.

The default implementation uses the internal AM decryption API to decode passwords. A custom implementation must implement the `com.sun.identity.saml.xmlsig.PasswordDecoder` interface.

Default value: `com.sun.identity.saml.xmlsig.FMPasswordDecoder`

amster attribute: `passwordDecoderClass`

SignatureProvider SPI implementation class

The Federation system uses this class to digitally sign SAML documents.

The default implementation uses the XERCES APIs to sign the documents. A custom implementation must implement the `com.sun.identity.saml.xmlsig.SignatureProvider` interface.

Default value: `com.sun.identity.saml.xmlsig.AMSignatureProvider`

amster attribute: `signatureProviderClass`

KeyProvider SPI implementation class

The Federation system uses this class to provide access to the underlying Java keystore.

The default implementation uses the Java Cryptographic Engine to provide access to the Java keystore. A custom implementation must implement the `com.sun.identity.saml.xmlsig.KeyProvider` interface.

Default value: `com.sun.identity.saml.xmlsig.JKSKeyProvider`

amster attribute: `keyProviderClass`

Algorithms

The following settings appear on the **Algorithms** tab:

XML canonicalization algorithm

The algorithm used to canonicalize XML documents.

The possible values for this property are:

- `http://www.w3.org/2001/10/xml-exc-c14n#`. i18n:famFederationCommon#http://www.w3.org/2001/10/xml-exc-c14n#
- `http://www.w3.org/2001/10/xml-exc-c14n#WithComments`. i18n:famFederationCommon#http://www.w3.org/2001/10/xml-exc-c14n#WithComments
- `http://www.w3.org/TR/2001/REC-xml-c14n-20010315`
- `http://www.w3.org/TR/2001/REC-xml-c14n-20010315#WithComments`. i18n:famFederationCommon#http://www.w3.org/TR/2001/REC-xml-c14n-20010315#WithComments

Default value: `http://www.w3.org/2001/10/xml-exc-c14n#`

amster attribute: `cannonicalizationAlgorithm`

XML signature algorithm

The algorithm used to sign XML documents.

The possible values for this property are:

- `http://www.w3.org/2000/09/xmldsig#rsa-sha1`. i18n:famFederationCommon#http://www.w3.org/2000/09/xmldsig#rsa-sha1
- `http://www.w3.org/2000/09/xmldsig#hmac-sha1`. i18n:famFederationCommon#http://www.w3.org/2000/09/xmldsig#hmac-sha1
- `http://www.w3.org/2000/09/xmldsig#dsa-sha1`. i18n:famFederationCommon#http://www.w3.org/2000/09/xmldsig#dsa-sha1

- `http://www.w3.org/2001/04/xmldsig-more#rsa-md5`. i18n:famFederationCommon#http://www.w3.org/2001/04/xmldsig-more#rsa-md5
- `http://www.w3.org/2001/04/xmldsig-more#rsa-ripemd160`. i18n:famFederationCommon#http://www.w3.org/2001/04/xmldsig-more#rsa-ripemd160
- `http://www.w3.org/2001/04/xmldsig-more#rsa-sha256`. i18n:famFederationCommon#http://www.w3.org/2001/04/xmldsig-more#rsa-sha256
- `http://www.w3.org/2001/04/xmldsig-more#rsa-sha384`. i18n:famFederationCommon#http://www.w3.org/2001/04/xmldsig-more#rsa-sha384
- `http://www.w3.org/2001/04/xmldsig-more#rsa-sha512`. i18n:famFederationCommon#http://www.w3.org/2001/04/xmldsig-more#rsa-sha512
- `http://www.w3.org/2001/04/xmldsig-more#hmac-md5`. i18n:famFederationCommon#http://www.w3.org/2001/04/xmldsig-more#hmac-md5
- `http://www.w3.org/2001/04/xmldsig-more#hmac-ripemd160`. i18n:famFederationCommon#http://www.w3.org/2001/04/xmldsig-more#hmac-ripemd160
- `http://www.w3.org/2001/04/xmldsig-more#hmac-sha256`. i18n:famFederationCommon#http://www.w3.org/2001/04/xmldsig-more#hmac-sha256
- `http://www.w3.org/2001/04/xmldsig-more#hmac-sha384`. i18n:famFederationCommon#http://www.w3.org/2001/04/xmldsig-more#hmac-sha384
- `http://www.w3.org/2001/04/xmldsig-more#hmac-sha512`. i18n:famFederationCommon#http://www.w3.org/2001/04/xmldsig-more#hmac-sha512

Default value: `http://www.w3.org/2001/04/xmldsig-more#rsa-sha256`

amster attribute: `signatureAlgorithm`

XML digest algorithm

The default digest algorithm to use in signing XML.

The possible values for this property are:

- `http://www.w3.org/2000/09/xmldsig#sha1`. i18n:famFederationCommon#http://www.w3.org/2000/09/xmldsig#sha1
- `http://www.w3.org/2001/04/xmlenc#sha256`. i18n:famFederationCommon#http://www.w3.org/2001/04/xmlenc#sha256
- `http://www.w3.org/2001/04/xmlenc#sha512`. i18n:famFederationCommon#http://www.w3.org/2001/04/xmlenc#sha512
- `http://www.w3.org/2001/04/xmldsig-more#sha384`. i18n:famFederationCommon#http://www.w3.org/2001/04/xmldsig-more#sha384

Default value: `http://www.w3.org/2001/04/xmlenc#sha256`

amster attribute: `DigestAlgorithm`

Query String signature algorithm (RSA)

The default signature algorithm to use in case of RSA keys.

The possible values for this property are:

- `http://www.w3.org/2000/09/xmldsig#rsa-sha1`. i18n:famFederationCommon#http://www.w3.org/2000/09/xmldsig#rsa-sha1
- `http://www.w3.org/2001/04/xmldsig-more#rsa-sha256`. i18n:famFederationCommon#http://www.w3.org/2001/04/xmldsig-more#rsa-sha256
- `http://www.w3.org/2001/04/xmldsig-more#rsa-sha384`. i18n:famFederationCommon#http://www.w3.org/2001/04/xmldsig-more#rsa-sha384
- `http://www.w3.org/2001/04/xmldsig-more#rsa-sha512`. i18n:famFederationCommon#http://www.w3.org/2001/04/xmldsig-more#rsa-sha512

Default value: `http://www.w3.org/2001/04/xmldsig-more#rsa-sha256`

amster attribute: `QuerySignatureAlgorithmRSA`

Query String signature algorithm (DSA)

The default signature algorithm to use in case of DSA keys.

The possible values for this property are:

- `http://www.w3.org/2000/09/xmldsig#dsa-sha1`. i18n:famFederationCommon#http://www.w3.org/2000/09/xmldsig#dsa-sha1
- `http://www.w3.org/2009/xmldsig11#dsa-sha256`. i18n:famFederationCommon#http://www.w3.org/2009/xmldsig11#dsa-sha256

Default value: `http://www.w3.org/2009/xmldsig11#dsa-sha256`

amster attribute: `QuerySignatureAlgorithmDSA`

Query String signature algorithm (EC)

The default signature algorithm to use in case of EC keys.

The possible values for this property are:

- `http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha1`. i18n:famFederationCommon#http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha1

- `http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha256`. i18n:famFederationCommon#http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha256
- `http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha384`. i18n:famFederationCommon#http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha384
- `http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha512`. i18n:famFederationCommon#http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha512

Default value: `http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha512`

amster attribute: `QuerySignatureAlgorithmEC`

XML transformation algorithm

The algorithm used to transform XML documents.

The possible values for this property are:

- `http://www.w3.org/2001/10/xml-exc-c14n#`. i18n:famFederationCommon#http://www.w3.org/2001/10/xml-exc-c14n#
- `http://www.w3.org/2001/10/xml-exc-c14n#WithComments`. i18n:famFederationCommon#http://www.w3.org/2001/10/xml-exc-c14n#WithComments
- `http://www.w3.org/TR/2001/REC-xml-c14n-20010315`
- `http://www.w3.org/TR/2001/REC-xml-c14n-20010315#WithComments`. i18n:famFederationCommon#http://www.w3.org/TR/2001/REC-xml-c14n-20010315#WithComments
- `http://www.w3.org/TR/1999/REC-xslt-19991116`
- `http://www.w3.org/2000/09/xmldsig#base64`. i18n:famFederationCommon#http://www.w3.org/2000/09/xmldsig#base64
- `http://www.w3.org/TR/1999/REC-xpath-19991116`
- `http://www.w3.org/2000/09/xmldsig#enveloped-signature`. i18n:famFederationCommon#http://www.w3.org/2000/09/xmldsig#enveloped-signature
- `http://www.w3.org/TR/2001/WD-xptr-20010108`
- `http://www.w3.org/2002/04/xmldsig-filter2`
- `http://www.w3.org/2002/06/xmldsig-filter2`
- `http://www.nue.et-inf.uni-siegen.de/~geuer-pollmann/#xpathFilter`. i18n:famFederationCommon#http://www.nue.et-inf.uni-siegen.de/~geuer-pollmann/#xpathFilter

Default value: `http://www.w3.org/2001/10/xml-exc-c14n#`

amster attribute: `transformationAlgorithm`

Mask Generation Function Algorithm

Which MGF algorithm to use when encrypting the symmetric encryption key using RSA OAEP algorithm.

The possible values for this property are:

- `http://www.w3.org/2009/xmlenc11#mgf1sha1`. i18n:famFederationCommon#http://www.w3.org/2009/xmlenc11#mgf1sha1
- `http://www.w3.org/2009/xmlenc11#mgf1sha224`. i18n:famFederationCommon#http://www.w3.org/2009/xmlenc11#mgf1sha224
- `http://www.w3.org/2009/xmlenc11#mgf1sha256`. i18n:famFederationCommon#http://www.w3.org/2009/xmlenc11#mgf1sha256
- `http://www.w3.org/2009/xmlenc11#mgf1sha384`. i18n:famFederationCommon#http://www.w3.org/2009/xmlenc11#mgf1sha384
- `http://www.w3.org/2009/xmlenc11#mgf1sha512`. i18n:famFederationCommon#http://www.w3.org/2009/xmlenc11#mgf1sha512

Default value: `http://www.w3.org/2009/xmlenc11#mgf1sha256`

amster attribute: `maskGenerationFunction`

AES Key Wrap Algorithm

Which AES key wrap algorithm to use when the remote entity provider does not specify which key wrap algorithm it supports.

The possible values for this property are:

- `http://www.w3.org/2001/04/xmlenc#kw-aes128`
- `http://www.w3.org/2001/04/xmlenc#kw-aes192`
- `http://www.w3.org/2001/04/xmlenc#kw-aes256`

Default value: `http://www.w3.org/2001/04/xmlenc#kw-aes256`

amster attribute: `aesKeyWrapAlgorithm`

RSA Key Transport Algorithm

The possible values for this property are:

- `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`

Default value: `http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p`

amster attribute: `rsaKeyTransportAlgorithm`

Monitoring

The following settings appear on the **Monitoring** tab:

Monitoring Agent Provider Class

The Federation system uses this class to gain access to the monitoring system.

The default implementation uses the built-in AM monitoring system. A custom implementation must implement the `com.sun.identity.plugin.monitoring.FedMonAgent` interface.

Default value: `com.sun.identity.plugin.monitoring.impl.AgentProvider`

amster attribute: `monitoringAgentClass`

Monitoring Provider Class for SAML2

The SAML2 engine uses this class to gain access to the monitoring system.

The default implementation uses the built-in AM monitoring system. A custom implementation must implement the `com.sun.identity.plugin.monitoring.FedMonSAML2Svc` interface.

Default value: `com.sun.identity.plugin.monitoring.impl.FedMonSAML2SvcProvider`

amster attribute: `monitoringSaml2Class`

Configuration Version Service

amster service name: `ConfigurationVersionService`

The following settings are available in this service:

configurationCommit

amster attribute: `configurationCommit`

Configuration Version

AM's configuration version

Default value: `3.0.0.1`

amster attribute: `configurationVersion`

CORS Service

amster service name: `CorsConfiguration`

Configuration

The following settings appear on the **Configuration** tab:

Enable the CORS filter

If disable, no CORS headers will be added to responses.

Default value: `true`

amster attribute: `enabled`

Secondary Configurations

This service has the following Secondary Configurations.

configuration

Enable the CORS filter

If disable, no CORS headers will be added to responses.

Default value: `false`

amster attribute: `enabled`

Accepted Origins

The set of accepted origins.

amster attribute: `acceptedOrigins`

Accepted Methods

The set of (non-simple) accepted methods, included in the pre-flight response in the header Access-Control-Allow-Methods.

amster attribute: `acceptedMethods`

Accepted Headers

The set of (non-simple) accepted headers, included in the pre-flight response in the header Access-Control-Allow-Headers.

amster attribute: `acceptedHeaders`

Exposed Headers

The set of headers to transmit in the header Access-Control-Expose-Headers.

amster attribute: `exposedHeaders`

Max Age

The max age (in seconds) for caching, included in the pre-flight response in the header Access-Control-Max-Age.

Default value: `0`

amster attribute: `maxAge`

Allow Credentials

Whether to transmit the Access-Control-Allow-Credentials: true header in the response.

Default value: `false`

amster attribute: `allowCredentials`

Dashboard

amster service name: `DashboardUserService`

Realm Defaults

The following settings appear on the **Realm Defaults** tab:

Available Dashboard Apps

List of application dashboard names available by default for realms with the Dashboard service configured.

amster attribute: `assignedDashboard`

Secondary Configurations

This service has the following Secondary Configurations.

instances

Dashboard Class Name

Identifies how to access the application, for example `SAML2ApplicationClass` for a SAML v2.0 application.

amster attribute: `className`

Dashboard Name

The application name as it will appear to the administrator for configuring the dashboard.

amster attribute: `name`

Dashboard Display Name

The application name that displays on the dashboard client.

amster attribute: `displayName`

Dashboard Icon

The icon name that will be displayed on the dashboard client identifying the application.

amster attribute: `icon`

Dashboard Login

The URL that takes the user to the application.

amster attribute: `login`

ICF Identifier

amster attribute: `icfIdentifier`

Device ID Service

amster service name: `deviceIdService`

Realm Defaults

The following settings appear on the **Realm Defaults** tab:

Profile Storage Attribute

The user's attribute in which to store Device ID profiles.

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 enabling the Device ID authentication module. AM must be able to write to the attribute.

Default value: `devicePrintProfiles`

amster attribute: `deviceIdAttrName`

Device Profile Encryption Scheme

Encryption scheme to use to secure device profiles stored on the server.

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.

Note: AES-256 may require installation of the JCE Unlimited Strength policy files.

The possible values for this property are:

- Label: **AES-256/HMAC-SHA-512 with RSA Key Wrapping** (Value: `RSAES_AES256CBC_HS512`)
- Label: **AES-128/HMAC-SHA-256 with RSA Key Wrapping** (Value: `RSAES_AES128CBC_HS256`)
- Label: **No encryption of device settings.** (Value: `NONE`)

Default value: `NONE`

amster attribute: `deviceIdSettingsEncryptionScheme`

Encryption Key Store

Path to the key store from which to load encryption keys.

Default value: `/path/to/openam/security/keystores/keystore.jks`

amster attribute: `deviceIdSettingsEncryptionKeystore`

Key Store Type

Type of key store to load.

Note: 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.

See the JDK 8 PKCS#11 Reference Guide for more details.

The possible values for this property are:

- Label: **Java Key Store (JKS).** (Value: `JKS`)

- Label: **Java Cryptography Extension Key Store (JCEKS).** (Value: `JCEKS`)
- Label: **PKCS#11 Hardware Crypto Storage.** (Value: `PKCS11`)
- Label: **PKCS#12 Key Store.** (Value: `PKCS12`)

Default value: `JKS`

amster attribute: `deviceIdSettingsEncryptionKeystoreType`

Key Store Password

Password to unlock the key store. This password is encrypted when it is saved in the AM configuration. You should modify the default value.

amster attribute: `deviceIdSettingsEncryptionKeystorePassword`

Key-Pair Alias

Alias of the certificate and private key in the key store. The private key is used to encrypt and decrypt device profiles.

amster attribute: `deviceIdSettingsEncryptionKeystoreKeyPairAlias`

Private Key Password

Password to unlock the private key.

amster attribute: `deviceIdSettingsEncryptionKeystorePrivateKeyPassword`

Device Profiles Service

amster service name: `DeviceProfilesService`

Realm Defaults

The following settings appear on the **Realm Defaults** tab:

Profile Storage Attribute

The user's attribute in which to store Device profiles.

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 enabling the Device Profiles authentication module. AM must be able to write to the attribute.

Default value: `deviceProfiles`

amster attribute: `deviceProfilesAttrName`

Device Profile Encryption Scheme

Encryption scheme to use to secure device profiles stored on the server.

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.

Note: AES-256 may require installation of the JCE Unlimited Strength policy files.

The possible values for this property are:

- Label: **AES-256/HMAC-SHA-512 with RSA Key Wrapping** (Value: `RSAES_AES256CBC_HS512`)
- Label: **AES-128/HMAC-SHA-256 with RSA Key Wrapping** (Value: `RSAES_AES128CBC_HS256`)
- Label: **No encryption of device settings.** (Value: `NONE`)

Default value: `NONE`

amster attribute: `deviceProfilesSettingsEncryptionScheme`

Encryption Key Store

Path to the key store from which to load encryption keys.

Default value: `/path/to/openam/security/keystores/keystore.jks`

amster attribute: `deviceProfilesSettingsEncryptionKeystore`

Key Store Type

Type of key store to load.

Note: 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.

See the JDK 8 PKCS#11 Reference Guide for more details.

The possible values for this property are:

- Label: **Java Key Store (JKS).** (Value: `JKS`)
- Label: **Java Cryptography Extension Key Store (JCEKS).** (Value: `JCEKS`)
- Label: **PKCS#11 Hardware Crypto Storage.** (Value: `PKCS11`)
- Label: **PKCS#12 Key Store.** (Value: `PKCS12`)

Default value: `JKS`

amster attribute: `deviceProfilesSettingsEncryptionKeystoreType`

Key Store Password

Password to unlock the key store. This password is encrypted when it is saved in the AM configuration. You should modify the default value.

amster attribute: `deviceProfilesSettingsEncryptionKeystorePassword`

Key-Pair Alias

Alias of the certificate and private key in the key store. The private key is used to encrypt and decrypt device profiles.

amster attribute: `deviceProfilesSettingsEncryptionKeystoreKeyPairAlias`

Private Key Password

Password to unlock the private key.

amster attribute: `deviceProfilesSettingsEncryptionKeystorePrivateKeyPassword`

Email Service

amster service name: `EmailService`

Realm Defaults

The following settings appear on the **Realm Defaults** tab:

Email Message Implementation Class

Specifies the class that sends email notifications, such as those sent for user registration and forgotten passwords.

Default value: `org.forgerock.openam.services.email.MailServerImpl`

amster attribute: `emailImplClassName`

Mail Server Host Name

Specifies the fully qualified domain name of the SMTP mail server through which to send email notifications.

For example, you might set this property to: *smtp.example.com*

amster attribute: `hostname`

Mail Server Host Port

Specifies the port number for the SMTP mail server.

Default value: `465`

amster attribute: `port`

Mail Server Authentication Username

Specifies the user name for the SMTP mail server.

For example, you might set this property to: *username*

amster attribute: `username`

Mail Server Authentication Password

Specifies the password for the SMTP user name.

amster attribute: `password`

Mail Server Secure Connection

Specifies whether to connect to the SMTP mail server using SSL.

The possible values for this property are:

- `SSL`
- `Non SSL`
- `Start TLS`

Default value: `SSL`

amster attribute: `sslState`

Email From Address

Specifies the address from which to send email notifications.

For example, you might set this property to: *no-reply@example.com*

amster attribute: `from`

Email Attribute Name

Specifies the profile attribute from which to retrieve the end user's email address.

Default value: `mail`

amster attribute: `emailAddressAttribute`

Email Subject

Specifies a subject for notification messages. If you do not set this, AM does not set the subject for notification messages.

amster attribute: `subject`

Email Content

Specifies content for notification messages. If you do not set this, AM includes only the confirmation URL in the mail body.

amster attribute: `message`

Email Rate Limit

Specifies the minimum number of seconds which must elapse between sending emails to an individual user.

Default value: `1`

amster attribute: `emailRateLimitSeconds`

External Data Stores

amster service name: `DataStoreService`

Realm Defaults

The following settings appear on the **Realm Defaults** tab:

Policy Data Store

Select a data store configuration to be used for policy storage

The possible values for this property are:

- Label: **Default Data Store** (Value: `fd270e31-1788-4193-8734-eb2d500c47f3`)

Default value: `fd270e31-1788-4193-8734-eb2d500c47f3`

amster attribute: `policyDataStoreId`

Application Data Store

Select a data store configuration to be used for application storage

The possible values for this property are:

- Label: **Default Data Store** (Value: `fd270e31-1788-4193-8734-eb2d500c47f3`)

Default value: `fd270e31-1788-4193-8734-eb2d500c47f3`

amster attribute: `applicationDataStoreId`

Secondary Configurations

This service has the following Secondary Configurations.

config

Host Urls

An ordered list of connection strings for LDAP directories.Each connection string is composed as follows: HOST:PORT. serverHostname = Host Name

amster attribute: `serverUrls`

Bind DN

amster attribute: `bindDN`

Bind Password

amster attribute: `bindPassword`

Minimum Connection Pool Size

Default value: `1`

amster attribute: `minimumConnectionPool`

Maximum Connection Pool Size

Default value: `10`

amster attribute: `maximumConnectionPool`

Use SSL

amster attribute: `useSsl`

Start TLS

amster attribute: `useStartTLS`

Affinity Enabled

amster attribute: `affinityEnabled`

ForgeRock Authenticator (OATH) Service

amster service name: `AuthenticatorOath`

Realm Defaults

The following settings appear on the **Realm Defaults** tab:

Profile Storage Attribute

Attribute for storing ForgeRock Authenticator OATH profiles.

The default attribute is added to the user store during AM 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 AM. AM must be able to write to the attribute.

Default value: `oathDeviceProfiles`

amster attribute: `oathAttrName`

Device Profile Encryption Scheme

Encryption scheme for securing device profiles stored on the server.

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.

Note: AES-256 may require installation of the JCE Unlimited Strength policy files.

The possible values for this property are:

- Label: **AES-256/HMAC-SHA-512 with RSA Key Wrapping** (Value: `RSAES_AES256CBC_HS512`)
- Label: **AES-128/HMAC-SHA-256 with RSA Key Wrapping** (Value: `RSAES_AES128CBC_HS256`)
- Label: **No encryption of device settings.** (Value: `NONE`)

Default value: `NONE`

amster attribute: `authenticatorOATHDeviceSettingsEncryptionScheme`

Encryption Key Store

Path to the key store from which to load encryption keys.

Default value: `/path/to/openam/openam/keystore.jks`

amster attribute: `authenticatorOATHDeviceSettingsEncryptionKeystore`

Key Store Type

Type of encryption key store.

Note: 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.

See the JDK 8 PKCS#11 Reference Guide for more details.

The possible values for this property are:

- Label: **Java Key Store (JKS).** (Value: `JKS`)
- Label: **Java Cryptography Extension Key Store (JCEKS).** (Value: `JCEKS`)
- Label: **PKCS#11 Hardware Crypto Storage.** (Value: `PKCS11`)
- Label: **PKCS#12 Key Store.** (Value: `PKCS12`)

Default value: `JKS`

amster attribute: `authenticatorOATHDeviceSettingsEncryptionKeystoreType`

Key Store Password

Password to unlock the key store. This password will be encrypted.

amster attribute: `authenticatorOATHDeviceSettingsEncryptionKeystorePassword`

Key-Pair Alias

Alias of the certificate and private key in the key store. The private key is used to encrypt and decrypt device profiles.

Default value: `pushDeviceProfiles`

amster attribute: `authenticatorOATHDeviceSettingsEncryptionKeystoreKeyPairAlias`

Private Key Password

Password to unlock the private key.

amster attribute: `authenticatorOATHDeviceSettingsEncryptionKeystorePrivateKeyPassword`

ForgeRock Authenticator (OATH) Device Skippable Attribute Name

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 writable.

Default value: `oath2faEnabled`

amster attribute: `authenticatorOATHSkippableName`

ForgeRock Authenticator (Push) Service

amster service name: `AuthenticatorPush`

Realm Defaults

The following settings appear on the **Realm Defaults** tab:

Profile Storage Attribute

The user's attribute in which to store Push Notification profiles.

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 push notifications with the ForgeRock Authenticator app in AM. AM must be able to write to the attribute.

Default value: `pushDeviceProfiles`

amster attribute: `pushAttrName`

Device Profile Encryption Scheme

Encryption scheme to use to secure device profiles stored on the server.

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.

Note: AES-256 may require installation of the JCE Unlimited Strength policy files.

The possible values for this property are:

- Label: **AES-256/HMAC-SHA-512 with RSA Key Wrapping** (Value: `RSAES_AES256CBC_HS512`)
- Label: **AES-128/HMAC-SHA-256 with RSA Key Wrapping** (Value: `RSAES_AES128CBC_HS256`)
- Label: **No encryption of device settings.** (Value: `NONE`)

Default value: `NONE`

amster attribute: `authenticatorPushDeviceSettingsEncryptionScheme`

Encryption Key Store

Path to the key store from which to load encryption keys.

Default value: `/path/to/openam/openam/keystore.jks`

amster attribute: `authenticatorPushDeviceSettingsEncryptionKeystore`

Key Store Type

Type of key store to load.

Note: 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.

See the JDK 8 PKCS#11 Reference Guide for more details.

The possible values for this property are:

- Label: **Java Key Store (JKS).** (Value: `JKS`)
- Label: **Java Cryptography Extension Key Store (JCEKS).** (Value: `JCEKS`)
- Label: **PKCS#11 Hardware Crypto Storage.** (Value: `PKCS11`)
- Label: **PKCS#12 Key Store.** (Value: `PKCS12`)

Default value: `JKS`

amster attribute: `authenticatorPushDeviceSettingsEncryptionKeystoreType`

Key Store Password

Password to unlock the key store. This password is encrypted when it is saved in the AM configuration. You should modify the default value.

amster attribute: `authenticatorPushDeviceSettingsEncryptionKeystorePassword`

Key-Pair Alias

Alias of the certificate and private key in the key store. The private key is used to encrypt and decrypt device profiles.

amster attribute: `authenticatorPushDeviceSettingsEncryptionKeystoreKeyPairAlias`

Private Key Password

Password to unlock the private key.

amster attribute: `authenticatorPushDeviceSettingsEncryptionKeystorePrivateKeyPassword`

ForgeRock Authenticator (Push) Device Skippable Attribute Name

Name of the attribute on a user's profile used to store their selection of whether to skip ForgeRock Authenticator (Push) 2FA modules.

Default value: `push2faEnabled`

amster attribute: `authenticatorPushSkippableName`

Globalization Settings

amster service name: `Globalization`

Global Attributes

The following settings appear on the **Global Attributes** tab:

Charsets Supported by Each Locale

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.

Default value:

```
locale=zh|charset=UTF-8;GB2312
locale=ar|charset=UTF-8;ISO-8859-6
locale=es|charset=UTF-8;ISO-8859-15
locale=de|charset=UTF-8;ISO-8859-15
locale=zh_TW|charset=UTF-8;BIG5
locale=fr|charset=UTF-8;ISO-8859-15
locale=ko|charset=UTF-8;EUC-KR
locale=en|charset=UTF-8;ISO-8859-1
locale=th|charset=UTF-8;TIS-620
locale=ja|charset=UTF-8;Shift_JIS;EUC-JP
```

amster attribute: `charsetMappings`

Charset Aliases

Use this list to map between different character set names used in Java and in MIME.

Default value:

```
mimeName=EUC-KR|javaName=EUC_KR
mimeName=EUC-JP|javaName=EUC_JP
mimeName=Shift_JIS|javaName=SJIS
```

amster attribute: `sun-identity-g11n-settings-charset-alias-mapping`

Realm Defaults

The following settings appear on the **Realm Defaults** tab:

Auto Generated Common Name Format

Use this list to configure how AM formats names shown in the console banner.

This setting allows the name of the authenticated user shown in the AM console banner to be customised based on the locale of the user.

Default value: `zh={sn}{givenname}`

amster attribute: `commonNameFormats`

Google Cloud Platform Service Accounts

amster service name: `GoogleCloudServiceAccountService`

Secondary Configurations

This service has the following Secondary Configurations.

serviceAccounts

Credentials Secret ID

The ID of the secret that contains the GCP service account credentials. Leave blank to usethe default credentials from the environment. Credentials can be loaded from disk using a FileSystem Secret Store.

amster attribute: `credentialsSecretId`

Allowed Realms

A list of realms that are allowed to use this service account. Realms should be specified in path form, such as `/subrealm/subsubrealm`.

amster attribute: `allowedRealms`

Allowed Secret Names

A list of patterns of Google Secret Manager secret names that are allowed to be usedwith this service account. Patterns can include the wildcard "*".

Default value: `*`

amster attribute: `allowedSecretNamePatterns`

Disallowed Secret Names

A list of patterns of Google Secret Manager secret names that are *not* allowed to be used with this service account. Patterns can include the wildcard "*".

amster attribute: `disallowedSecretNamePatterns`

IDM Provisioning

amster service name: `IDMProvisioning`

The following settings are available in this service:

Enabled

Default value: `false`

amster attribute: `enabled`

Deployment URL

URL of the IDM deployment, e.g. https://localhost:8080

amster attribute: `idmDeploymentUrl`

Deployment Path

Path of the IDM deployment, e.g. openidm

amster attribute: `idmDeploymentPath`

IDM Provisioning Client

The name of the oauth client to be used for the client credentials flow

amster attribute: `idmProvisioningClient`

Signing Key Alias

Alias of the signing symmetric key in AM's default keystore. Must be a duplicate of the symmetric key used by IDM.

amster attribute: `provisioningSigningKeyAlias`

Encryption Key Alias

Alias of the encryption asymmetric key in AM's default keystore. Must be a duplicate of the asymmetric key used by IDM.

amster attribute: `provisioningEncryptionKeyAlias`

Signing Algorithm

JWT signing algorithm.

amster attribute: `provisioningSigningAlgorithm`

Signing Compatibility Mode

Enable AM to communicate with OpenIDM 6 and earlier.

When this option is enabled, AM 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.

Default value: `false`

amster attribute: `jwtSigningCompatibilityMode`

Encryption Algorithm

JWT encryption algorithm.

amster attribute: `provisioningEncryptionAlgorithm`

Encryption Method

JWT encryption method.

amster attribute: `provisioningEncryptionMethod`

IoT Service

amster service name: `IoTService`

Realm Defaults

The following settings appear on the **Realm Defaults** tab:

Create OAuth 2.0 Client

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).

Default value: `false`

amster attribute: `createOAuthClient`

OAuth 2.0 Client Name

The name of the default OAuth 2.0 Client used by the IoT Service to request access tokens for things.

Default value: `forgerock-iot-oauth2-client`

amster attribute: `oauthClientName`

Create OAuth 2.0 JWT Issuer

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.

Default value: `false`

amster attribute: `createOAuthJwtIssuer`

OAuth 2.0 JWT Issuer Name

The name of the Trusted JWT Issuer used by the IoT Service to request access tokens for things.

Default value: `forgerock-iot-jwt-issuer`

amster attribute: `oauthJwtIssuerName`

OAuth 2.0 Subject Attribute

The name of the identity store attribute from which to read the OAuth 2.0 subject value. The subject is used in access tokens issued for things. This allows the thing's access token subject to have a value other than the thing's ID, which is the value used by default.

amster attribute: `oauthSubjectAttribute`

Readable Attributes

Specifies the list of attributes that a thing is allowed to request from its identity.

Default value: `thingConfig`

amster attribute: `attributeAllowlist`

Legacy User Self Service

amster service name: `SecurityProperties`

Realm Defaults

The following settings appear on the **Realm Defaults** tab:

Legacy Self-Service REST Endpoint

Specify whether to enable the legacy self-service endpoint.

AM supports two User Self-Service components: the Legacy User Self-Service, which is based on a Java SDK and is available in AM versions prior to AM 13, and a common REST-based/XUI-based User Self-Service available in AM 13 and later.

The Legacy User Self-Service will be deprecated in a future release.

Default value: `false`

amster attribute: `selfServiceEnabled`

Self-Registration for Users

If enabled, new users can sign up using a REST API client.

Default value: `false`

amster attribute: `selfRegistrationEnabled`

Self-Registration Token LifeTime (seconds)

Maximum life time for the token allowing User Self-Registration using the REST API.

Default value: `900`

amster attribute: `selfRegistrationTokenLifetime`

Self-Registration Confirmation Email URL

This page handles the HTTP GET request when the user clicks the link sent by email in the confirmation request.

Default value: `http://openam.example.com:8080/openam/XUI/confirm.html`

amster attribute: `selfRegistrationConfirmationUrl`

Forgot Password for Users

If enabled, users can assign themselves a new password using a REST API client.

Default value: `false`

amster attribute: `forgotPasswordEnabled`

Forgot Password Token Lifetime (seconds)

Maximum life time for the token that allows a user to process a forgotten password using the REST API.

Default value: `900`

amster attribute: `forgotPasswordTokenLifetime`

Forgot Password Confirmation Email URL

This page handles the HTTP GET request when the user clicks the link sent by email in the confirmation request.

Default value: `http://openam.example.com:8080/openam/XUI/confirm.html`

amster attribute: `forgotPasswordConfirmationUrl`

Destination After Successful Self-Registration

Specifies the behavior when self-registration has successfully completed.

The possible values for this property are:

- Label: **User is sent to a 'successful registration' page, without being logged in.** (Value: `default`)
- Label: **User is sent to the login page, to authenticate.** (Value: `login`)
- Label: **User is automatically logged in and sent to the appropriate page within the system.** (Value: `autologin`)

Default value: `default`

amster attribute: `userRegisteredDestination`

Protected User Attributes

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.

amster attribute: `protectedUserAttributes`

Confirmation Id HMAC Signing Key

256-bit key (base64-encoded) to use for HMAC signing of the legacy self-service confirmation email links.

Default value: `Bn+TrDWLSv1E3ADHWxgqpv4fZnVmKLqwQcZvGdo/3jU=`

amster attribute: `confirmationIdHmacKey`

Logging

amster service name: `Logging`

General

The following settings appear on the **General** tab:

Log Status

Enable the AM logging system.

AM supports two Audit Logging Services: the legacy Logging Service, which is based on a Java SDK and is available in AM versions prior to AM 13.5, and a new common REST-based Audit Logging Service available from AM 13.5.

The legacy Logging Service will be deprecated in a future release.

The possible values for this property are:

- `ACTIVE`
- `INACTIVE`

Default value: `INACTIVE`

amster attribute: `status`

Logging Type

Specifies whether to log to a database, Syslog, or to the filing system.

If you choose database then be sure to set the connection attributes correctly, including the JDBC driver to use.

The possible values for this property are:

- `File`
- `DB`
- `Syslog`

Default value: `File`

amster attribute: `type`

Configurable Log Fields

Controls the fields that are logged by AM.

This property is the list of fields that are logged by default. Administrators can choose to limit the information logged by AM.

Default value:

```
IPAddr
LoggedBy
LoginID
NameID
ModuleName
ContextID
Domain
LogLevel
HostName
MessageID
```

amster attribute: `fields`

Log Verification Frequency

The frequency (in seconds) that AM verifies security of the log files.

When secure logging is enabled, this is the period that AM will check the integrity of the log files.

Default value: `3600`

amster attribute: `verifyPeriod`

Log Signature Time

The frequency (in seconds) that AM will digitally sign the log records.

When secure logging is enabled, this is the period that AM will digitally signed the contents of the log files. The log signatures form the basis of the log file integrity checking.

Default value: `900`

amster attribute: `signaturePeriod`

Secure Logging

Enable or Disable secure logging.

Enabling this setting will cause AM 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.

The possible values for this property are:

- `ON`
- `OFF`

Default value: `OFF`

amster attribute: `security`

Secure Logging Signing Algorithm

Determines the algorithm used to digitally sign the log records.

The possible values for this property are:

- `MD2withRSA`. MD2 with RSA
- `MD5withRSA`. MD5 with RSA
- `SHA1withDSA`. SHA1 with DSA
- `SHA1withRSA`. SHA1 with RSA

Default value: `SHA1withRSA`

amster attribute: `signingAlgorithm`

Logging Certificate Store Location

The path to the Java keystore containing the logging system certificate.

The secure logging system will use the certificate alias of `Logger` to locate the certificate in the specified keystore.

Default value: `%BASE_DIR%/var/audit/Logger.jks`

amster attribute: `certificateStore`

Number of Files per Archive

Controls the number of logs files that will be archived by the secure logging system.

Default value: `5`

amster attribute: `filesPerKeystore`

Buffer Size

The number of log records held in memory before the log records will be flushed to the logfile or the database.

Default value: `25`

amster attribute: `bufferSize`

Buffer Time

The maximum time (in seconds) AM will hold log records in memory before flushing to the underlying repository.

Default value: `60`

amster attribute: `bufferTime`

Time Buffering

Enable or Disable log buffering

When enabled AM holds all log records in a memory buffer that it periodically flush to the repository. The period is set in the *Buffer Time* property.

The possible values for this property are:

- `ON`
- `OFF`

Default value: `ON`

amster attribute: `buffering`

Logging Level

Control the level of JDK logging within AM.

The possible values for this property are:

- `OFF`
- `SEVERE`
- `WARNING`
- `INFO`
- `CONFIG`
- `FINE`
- `FINER`
- `FINEST`

Default value: `INFO`

amster attribute: `jdkLoggingLevel`

File

The following settings appear on the **File** tab:

Log Rotation

Enable log rotation to cause new log files to be created when configured thresholds are reached, such as *Maximum Log Size* or *Logfile Rotation Interval*.

Default value: `true`

amster attribute: `rotationEnabled`

Maximum Log Size

Maximum size of a log file, in bytes.

Default value: `100000000`

amster attribute: `maxFileSize`

Number of History Files

Sets the number of history files for each log that AM keeps, including time-based histories.

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.

For time-based logs, a new set of logs will be created when AM is started because of the time-based file names that are used.

Default value: `1`

amster attribute: `numberHistoryFiles`

Logfile Rotation Prefix

The name of the log files will be prefixed with the supplied value.

This field defines the log file prefix. The prefix will be added to the name of all logfiles.

Note: Only used when time-based log rotation is enabled.

amster attribute: `prefix`

Logfile Rotation Suffix

The name of the log files will be suffixed with the supplied value.

This field defines the log file suffix. If no suffix is provided, then the following default suffix format will be used: `-MM.dd.yy-kk.mm`. The suffix allows use of Date and Time patterns defined in `SimpleDateFormat`

Note: This field is only used if the time based rotation is enabled.

Default value: `-MM.dd.yy-kk.mm`

amster attribute: `suffix`

Logfile Rotation Interval

The rotation interval (in minutes).

The rotation interval determines the frequency of when the log files will be rotated. If the value is `-1`, then time based rotation is disabled and log file size based rotation is enabled.

Default value: `-1`

amster attribute: `rotationInterval`

Log File Location

The path to the location of the log files

This property controls the location of the log files; the value of this property varies on whether File or DB logging is in use:

- File: The full pathname to the directory containing the log files.
- DB: The JDBC URL to the database used to store the log file database.

Default value: `%BASE_DIR%/var/audit/`

amster attribute: `location`

Database

The following settings appear on the **Database** tab:

Database User Name

When logging to a database, set this to the user name used to connect to the database. If this attribute is incorrectly set, AM performance suffers.

Default value: `dbuser`

amster attribute: `user`

Database User Password

When logging to a database, set this to the password used to connect to the database. If this attribute is incorrectly set, AM performance suffers.

amster attribute: `password`

Database Driver Name

When logging to a database, set this to the class name of the JDBC driver used to connect to the database.

The default is for Oracle. AM also works with the MySQL database driver.

Default value: `oracle.jdbc.driver.OracleDriver`

amster attribute: `driver`

Maximum Number of Records

The maximum number of records read from the logs via the Logging API

Default value: `500`

amster attribute: `maxRecords`

DB Failure Memory Buffer Size

Max number of log records held in memory if DB logging fails.

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. AM monitoring records the number of log entries cleared when the database was unavailable.

If the value of this property is less than that of the *Buffer Size* then the buffer size value will take precedence.

Default value: `2`

amster attribute: `databaseFailureMemoryBufferSize`

Syslog

The following settings appear on the **Syslog** tab:

Syslog server host

The URL or IP address of the syslog server, for example `http://mysyslog.example.com`, or `localhost`.

Default value: `localhost`

amster attribute: `host`

Syslog server port

The port number the syslog server is configured to listen to.

Default value: `514`

amster attribute: `port`

Syslog transport protocol

The protocol to use to connect to the syslog server.

The possible values for this property are:

- `UDP`
- `TCP`

Default value: `UDP`

amster attribute: `protocol`

Syslog facility

Syslog uses the facility level to determine the type of program that is logging the message.

The possible values for this property are:

- `kern`
- `user`
- `mail`
- `daemon`
- `auth`
- `syslog`
- `lpr`
- `news`
- `uucp`
- `cron`
- `authpriv`
- `ftp`
- `local0`
- `local1`

- `local2`
- `local3`
- `local4`
- `local5`
- `local6`
- `local7`

Default value: `local5`

amster attribute: `facility`

Syslog connection timeout

The amount of time to wait when attempting to connect to the syslog server before reporting a failure, in seconds.

Default value: `30`

amster attribute: `timeout`

Monitoring

amster service name: `Monitoring`

Configuration

The following settings appear on the **Configuration** tab:

Monitoring Status

Enable / Disable the monitoring system

Default value: `false`

amster attribute: `enabled`

Monitoring HTTP Port

Port number for the HTTP monitoring interface

Default value: `8082`

amster attribute: `httpPort`

Monitoring HTTP interface status

Enable / Disable the HTTP access to the monitoring system

Default value: `false`

amster attribute: `httpEnabled`

Monitoring HTTP interface authentication file path

Path to the monitoring system authentication file

The `openam_mon_auth` file contains the username and password of the account used to protect the monitoring interfaces. The default username is `demo` with a password of `changeit`. Use the `ampassword` command to encrypt a new password.

Default value: `%BASE_DIR%/security/openam_mon_auth`

amster attribute: `authfilePath`

Monitoring RMI Port

Port number for the JMX monitoring interface

Default value: `9999`

amster attribute: `rmiPort`

Monitoring RMI interface status

Enable / Disable the JMX access to the monitoring system

Default value: `false`

amster attribute: `rmiEnabled`

Monitoring SNMP Port

Port number for the SNMP monitoring interface

Default value: `8085`

amster attribute: `snmpPort`

Monitoring SNMP interface status

Enable / Disable the SNMP access to the monitoring system

Default value: `false`

amster attribute: `snmpEnabled`

Policy evaluation monitoring history size

Size of the window of most recent policy evaluations to record to expose via monitoring system. Valid range is 100 - 1000000.

Default value: `10000`

amster attribute: `policyHistoryWindowSize`

Session monitoring history size

Size of the window of most recent session operations to record to expose via monitoring system. Valid range is 100 - 1000000.

Default value: `10000`

amster attribute: `sessionHistoryWindowSize`

Secondary Configurations

This service has the following Secondary Configurations.

crest

Enabled

Default value: `false`

amster attribute: `enabled`

graphite

Hostname

The hostname of the Graphite server to which metrics should be published.

amster attribute: `host`

Port

The port of the Graphite server to which metrics should be published.

Default value: `2004`

amster attribute: `port`

Frequency

The frequency (in seconds) at which metrics should be published.

Default value: `30`

amster attribute: `frequency`

prometheus

Enabled

Default value: `false`

amster attribute: `enabled`

Authentication Type

Default value: `BASIC`

amster attribute: `authenticationType`

Username

Default value: `prometheus`

amster attribute: `username`

Password

amster attribute: `password`

Multi-Federation Protocol

amster service name: `MultiFederationProtocol`

The following settings are available in this service:

Single Logout Handler List

List of Logout handlers for each supported federation protocol

The multi-federation protocol engine supports Single Logout. Each federation protocol requires a different single logout handler. Logout handler must implement the `com.sun.identity.multiprotocol.SingleLogoutHandler` interface.

Default value:

```
key=WSFED|class=com.sun.identity.multiprotocol.WSFederationSingleLogoutHandler
key=SAML2|class=com.sun.identity.multiprotocol.SAML2SingleLogoutHandler
```

amster attribute: `singleLogoutHandlerList`

Naming

amster service name: `Naming`

General Configuration

The following settings appear on the **General Configuration** tab:

Profile Service URL

Specifies the endpoint used by the profile service.

This attribute is deprecated.

Default value: `%protocol://%host:%port%uri/profileservice`

amster attribute: `profileUrl`

Session Service URL

Specifies the endpoint used by the session service.

Default value: `%protocol://%host:%port%uri/sessionservice`

amster attribute: `sessionUrl`

Logging Service URL

Specifies the endpoint used by the logging service.

Default value: `%protocol://%host:%port%uri/loggingservice`

amster attribute: `loggingUrl`

Policy Service URL

Specifies the endpoint used by the policy service.

Default value: `%protocol://%host:%port%uri/policyservice`

amster attribute: `policyUrl`

Authentication Service URL

Specifies the endpoint used by the authentication service.

Default value: `%protocol://%host:%port%uri/authservice`

amster attribute: `authUrl`

Federation Configuration

The following settings appear on the **Federation Configuration** tab:

SAML Web Profile/Artifact Service URL

Specifies the SAML v1 endpoint.

Default value: `%protocol://%host:%port%uri/SAMLAwareServlet`

amster attribute: `samlAwareServletUrl`

SAML SOAP Service URL

Specifies the SAML v1 SOAP service endpoint.

Default value: `%protocol://%host:%port%uri/SAMLSOAPReceiver`

amster attribute: `samlSoapReceiverUrl`

SAML Web Profile/POST Service URL

Specifies the SAML v1 Web Profile endpoint.

Default value: `%protocol://%host:%port%uri/SAMLPOSTProfileServlet`

amster attribute: `samlPostServletUrl`

SAML Assertion Manager Service URL

Specifies the SAML v1 assertion service endpoint.

Default value: `%protocol://%host:%port%uri/AssertionManagerServlet/AssertionManagerIF`

amster attribute: `samlAssertionManagerUrl`

JAXRPC Endpoint URL

Specifies the JAXRPC endpoint URL used by the remote IDM/SMS APIs.

Default value: `%protocol://%host:%port%uri/jaxrpc/`

amster attribute: `jaxrpcUrl`

Endpoint Configuration

The following settings appear on the **Endpoint Configuration** tab:

Identity Web Services Endpoint URL

Specifies the endpoint for the Identity WSDL services.

Default value: `%protocol://%host:%port%uri/identityservices/`

amster attribute: `jaxwsUrl`

Identity REST Services Endpoint URL

Specifies the endpoint for the Identity REST services.

Default value: `%protocol://%host:%port%uri/identity/`

amster attribute: `idsvcsRestUrl`

Security Token Service Endpoint URL

Specifies the STS endpoint.

Default value: `%protocol://%host:%port%uri/sts`

amster attribute: `stsUrl`

Security Token Service MEX Endpoint URL

Specifies the STS MEX endpoint.

Default value: `%protocol://%host:%port%uri/sts/mex`

amster attribute: `stsMexUrl`

OAuth2 Provider

amster service name: `OAuth2Provider`

Global Attributes

The following settings appear on the **Global Attributes** tab:

Token Blacklist Cache Size

Number of blacklisted tokens to cache in memory to speed up blacklist checks and reduce load on the CTS.

Default value: `10000`

amster attribute: `blacklistCacheSize`

Blacklist Poll Interval (seconds)

How frequently to poll for token blacklist changes from other servers, in seconds.

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.

Default value: `60`

amster attribute: `blacklistPollInterval`

Blacklist Purge Delay (minutes)

Length of time to blacklist tokens beyond their expiry time.

Allows additional time to account for clock skew to ensure that a token has expired before it is removed from the blacklist.

Default value: `1`

amster attribute: `blacklistPurgeDelay`

Client-Based Grant Token Upgrade Compatibility Mode

Enable AM to consume and create client-based OAuth 2.0 tokens in two different formats simultaneously.

Enable this option when upgrading AM 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 AM instances in the cluster have been upgraded.

Default value: `false`

amster attribute: `statelessGrantTokenUpgradeCompatibilityMode`

CTS Storage Scheme

Storage scheme to be used when storing OAuth2 tokens to CTS.

In order to support rolling upgrades, this should be set to the latest storage scheme supported by all AM instances within your cluster. Select the latest storage scheme once all AM instances in the cluster have been upgraded.

One-to-One Storage Scheme

Under this storage scheme, each OAuth2 token maps to an individual CTS entry.

This storage scheme is inefficient - use the Grant-Set Storage Scheme once all servers have been upgraded to a version which supports it.

Grant-Set Storage Scheme

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.

The possible values for this property are:

- Label: **One-to-One Storage Scheme** (Value: `CTS_ONE_TO_ONE_MODEL`)
- Label: **Grant-Set Storage Scheme** (Value: `CTS_GRANT_SET_MODEL`)

Default value: `CTS_ONE_TO_ONE_MODEL`

amster attribute: `storageScheme`

Enforce JWT Unreasonable Lifetime

Enable the enforcement of JWT token unreasonable lifetime during validation.

The JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants specification (https://datatracker.ietf.org/doc/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.

Default value: `true`

amster attribute: `jwtTokenLifetimeValidationEnabled`

JWT Unreasonable Lifetime (seconds)

Specify the lifetime (in seconds) of a JWT which should be considered unreasonable and rejected by validation.

The JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants specification (https://datatracker.ietf.org/doc/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.

Default value: `86400`

amster attribute: `jwtTokenUnreasonableLifetime`

Core

The following settings appear on the **Core** tab:

Use Client-Based Access & Refresh Tokens

When enabled, AM issues access and refresh tokens that can be inspected by resource servers.

Default value: `false`

amster attribute: `statelessTokensEnabled`

Use Macaroon Access and Refresh Tokens

When enabled, AM will issue access and refresh tokens as Macaroons with caveats.

Default value: `false`

amster attribute: `macaroonTokensEnabled`

Authorization Code Lifetime (seconds)

The time an authorization code is valid for, in seconds.

Default value: `120`

amster attribute: `codeLifetime`

Refresh Token Lifetime (seconds)

The time in seconds a refresh token is valid for. If this field is set to `-1`, the refresh token will never expire.

Default value: `604800`

amster attribute: `refreshTokenLifetime`

Access Token Lifetime (seconds)

The time an access token is valid for, in seconds. Note that if you set the value to `0`, the access token will not be valid. A maximum lifetime of 600 seconds is recommended.

Default value: `3600`

amster attribute: `accessTokenLifetime`

Issue Refresh Tokens

Whether to issue a refresh token when returning an access token.

Default value: `true`

amster attribute: `issueRefreshToken`

Issue Refresh Tokens on Refreshing Access Tokens

Whether to issue a refresh token when refreshing an access token.

Default value: `true`

amster attribute: `issueRefreshTokenOnRefreshedToken`

Use Policy Engine for Scope decisions

With this setting enabled, the policy engine is consulted for each scope value that is requested.

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.

Default value: `false`

amster attribute: `usePolicyEngineForScope`

OAuth2 Access Token Modification Script

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.

The possible values for this property are:

- Label: **OAuth2 Access Token Modification Script** (Value: `d22f9a0c-426a-4466-b95e-d0f125b0d5fa`)
- Label: **--- Select a script ---** (Value: `[Empty]`)

Default value: `d22f9a0c-426a-4466-b95e-d0f125b0d5fa`

amster attribute: `accessTokenModificationScript`

OAuth2 Access Token May Act Script

The script that is executed when issuing an access token explicitly to modify the `may_act` claim placed on the token.

The possible values for this property are:

- Label: **OAuth2 May Act Script** (Value: `c735de08-f8f2-4e69-aa4a-2d8d3d438323`)
- Label: **--- Select a script ---** (Value: `[Empty]`)

Default value: `[Empty]`

amster attribute: `accessTokenMayActScript`

OIDC ID Token May Act Script

The script that is executed when issuing an OIDC ID Token explicitly to modify the `may_act` claim placed on the token.

The possible values for this property are:

- Label: **OAuth2 May Act Script** (Value: `c735de08-f8f2-4e69-aa4a-2d8d3d438323`)
- Label: **--- Select a script ---** (Value: `[Empty]`)

Default value: `[Empty]`

amster attribute: `oidcMayActScript`

Advanced

The following settings appear on the **Advanced** tab:

Custom Login URL Template

Custom URL for handling login, to override the default AM login page.

Supports Freemarker syntax, with the following variables:

Variable	Description
`gotoUrl`	The URL to redirect to after login.
`acrValues`	The Authentication Context Class Reference (acr) values for the authorization request.
`realm`	The AM realm the authorization request was made on.
`module`	The name of the AM authentication module requested to perform resource owner authentication.
`service`	The name of the AM authentication chain requested to perform resource owner authentication.
`locale`	A space-separated list of locales, ordered by preference.

The following example template redirects users to a non-AM front end to handle login, which will then redirect back to the `/oauth2/authorize` endpoint with any required parameters:

```
http://mylogin.com/login?goto=${goto}<#if acrValues??>&acr_values=${acrValues}</#if><#if realm??
>&realm=${realm}</#if><#if module??>&module=${module}</#if><#if service??>&service=${service}</#if><#if
 locale??>&locale=${locale}</#if>
```

NOTE: Default AM login page is constructed using "Base URL Source" service.

amster attribute: `customLoginUrlTemplate`

Scope Implementation Class

The class that contains the required scope implementation, must implement the `org.forgerock.oauth2.core.ScopeValidator` interface.

Default value: `org.forgerock.openam.oauth2.OpenAMScopeValidator`

amster attribute: `scopeImplementationClass`

Response Type Plugins

List of plugins that handle the valid `response_type` values.

OAuth 2.0 clients pass response types as parameters to the OAuth 2.0 Authorization endpoint (`/oauth2/authorize`) to indicate which grant type is requested from the provider. For example, the client passes `code` when requesting an authorization code, and `token` when requesting an access token.

Values in this list take the form `response-type|plugin-class-name`.

Default value:

```
code|org.forgerock.oauth2.core.AuthorizationCodeResponseTypeHandler
id_token|org.forgerock.openidconnect.IdTokenResponseTypeHandler
device_code|org.forgerock.oauth2.core.TokenResponseTypeHandler
token|org.forgerock.oauth2.core.TokenResponseTypeHandler
```

amster attribute: `responseTypeClasses`

Additional Audience Values

The additional audience values that will be permitted when verifying Client Authentication JWTs.

These audience values will be in addition to the AS base, issuer and endpoint URIs.

amster attribute: `allowedAudienceValues`

Token Exchanger Plugins

List of plugins that handle the valid `requested_token_type` values.

When using the Token Exchange grant type, these handlers will be used to convert the provided `subject_token` and `actor_token` into the appropriate impersonation or delegation tokens for use with downstream services.

Default value:

```
urn:ietf:params:oauth:token-type:access_token=>urn:ietf:params:oauth:token-type:access_token|
org.forgerock.oauth2.core.tokenexchange.accesstoken.AccessTokenToAccessTokenExchanger
urn:ietf:params:oauth:token-type:id_token=>urn:ietf:params:oauth:token-type:id_token|
org.forgerock.oauth2.core.tokenexchange.idtoken.IdTokenToIdTokenExchanger
urn:ietf:params:oauth:token-type:access_token=>urn:ietf:params:oauth:token-type:id_token|
org.forgerock.oauth2.core.tokenexchange.accesstoken.AccessTokenToIdTokenExchanger
urn:ietf:params:oauth:token-type:id_token=>urn:ietf:params:oauth:token-type:access_token|
org.forgerock.oauth2.core.tokenexchange.idtoken.IdTokenToAccessTokenExchanger
```

amster attribute: `tokenExchangeClasses`

Token Validator Plugins

List of plugins that validate `subject_token` and `actor_token` values.

When using the Token Exchange grant type, these handlers will be used to convert the validate `subject_token` and `actor_token` values to ensure they meet the required criteria to be exchanged.

Default value:

```
urn:ietf:params:oauth:token-type:id_token|
org.forgerock.oauth2.core.tokenexchange.idtoken.OidcIdTokenValidator
urn:ietf:params:oauth:token-type:access_token|
org.forgerock.oauth2.core.tokenexchange.accesstoken.OAuth2AccessTokenValidator
```

amster attribute: `tokenValidatorClasses`

User Profile Attribute(s) the Resource Owner is Authenticated On

Names of profile attributes that resource owners use to log in. You can add others to the default, for example `mail`.

Default value: `uid`

amster attribute: `authenticationAttributes`

User Display Name attribute

The profile attribute that contains the name to be displayed for the user on the consent page.

Default value: `cn`

amster attribute: `displayNameAttribute`

Client Registration Scope Whitelist

The set of scopes allowed when registering clients dynamically, with translations.

Scopes may be entered as simple strings or pipe-separated strings representing the internal scope name, locale, and localized description.

For example: `read|en|Permission to view email messages in your account`

Locale strings are in the format: `language_country_variant`, for example `en`, `en_GB`, or `en_US_WIN`.

If the locale and pipe is omitted, the description is displayed to all users that have undefined locales.

If the description is also omitted, nothing is displayed on the consent page for the scope. For example specifying `read|` 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.

amster attribute: `supportedScopes`

Subject Types supported

List of subject types supported. Valid values are:

- `public` - Each client receives the same subject (`sub`) value.
- `pairwise` - Each client receives a different subject (`sub`) value, to prevent correlation between clients.

Default value:

```
public
pairwise
```

amster attribute: `supportedSubjectTypes`

Default Client Scopes

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 AM console.

amster attribute: `defaultScopes`

OAuth2 Token Signing Algorithm

Algorithm used to sign client-based OAuth 2.0 tokens in order to detect tampering.

AM supports signing algorithms listed in JSON Web Algorithms (JWA): "alg" (Algorithm) Header Parameter Values for JWS:

- `HS256` - HMAC with SHA-256.
- `HS384` - HMAC with SHA-384.
- `HS512` - HMAC with SHA-512.
- `ES256` - ECDSA with SHA-256 and NIST standard P-256 elliptic curve.
- `ES384` - ECDSA with SHA-384 and NIST standard P-384 elliptic curve.
- `ES512` - ECDSA with SHA-512 and NIST standard P-521 elliptic curve.
- `RS256` - RSASSA-PKCS-v1_5 using SHA-256.

The possible values for this property are:

- `HS256`
- `HS384`
- `HS512`
- `RS256`

- `RS384`
- `RS512`
- `ES256`
- `ES384`
- `ES512`
- `PS256`
- `PS384`
- `PS512`

Default value: `HS256`

amster attribute: `tokenSigningAlgorithm`

Client-Based Token Compression

Whether client-based access and refresh tokens should be compressed.

Default value: `false`

amster attribute: `tokenCompressionEnabled`

Encrypt Client-Based Tokens

Whether client-based access and refresh tokens should be encrypted.

Enabling token encryption will disable token signing as encryption is performed using direct symmetric encryption.

Default value: `false`

amster attribute: `tokenEncryptionEnabled`

Subject Identifier Hash Salt

If *pairwise* subject types are supported, it is *STRONGLY RECOMMENDED* to change this value. It is used in the salting of hashes for returning specific `sub` claims to individuals using the same `request_uri` or `sector_identifier_uri`.

Default value: `changeme`

amster attribute: `hashSalt`

Code Verifier Parameter Required

If enabled, requests using the authorization code grant require a `code_challenge` attribute.

For more information, read the PKCE specification.

Note that if a client specifies a `code_challenge` parameter in the authorization request, PKCE is enabled regardless of the value of this attribute.

The possible values for this property are:

- Label: **All requests** (Value: `true`)
- Label: **Requests from all public clients** (Value: `public`)
- Label: **Requests from all passwordless public clients** (Value: `passwordless`)
- Label: **No requests** (Value: `false`)

Default value: `false`

amster attribute: `codeVerifierEnforced`

Modified Timestamp Attribute Name

The identity Data Store attribute used to return modified timestamp values.

This attribute is paired together with the *Created Timestamp Attribute Name* attribute (`createdTimestampAttribute`). 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.

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 `userinfo` endpoint to obtain the `updated_at` claim value in the ID token. The `updated_at` claim obtains its value from the `modifiedTimestampAttribute` attribute in the user profile. If the profile has never been modified the `updated_at` claim uses the `createdTimestampAttribute` attribute.

amster attribute: `modifiedTimestampAttribute`

Created Timestamp Attribute Name

The identity Data Store attribute used to return created timestamp values.

amster attribute: `createdTimestampAttribute`

Password Grant Authentication Service

The authentication service (chain or tree) that will be used to authenticate the username and password for the resource owner password credentials grant type.

The possible values for this property are:

- `[Empty]`
- `ldapService`

- `amsterService`
- `Example`
- `Agent`
- `RetryLimit`
- `PersistentCookie`
- `HmacOneTimePassword`
- `Facebook-ProvisionIDMAccount`
- `Google-AnonymousUser`
- `Google-DynamicAccountCreation`
- `PlatformRegistration`
- `PlatformProgressiveProfile`
- `PlatformLogin`
- `PlatformForgottenUsername`
- `PlatformResetPassword`
- `PlatformUpdatePassword`

amster attribute: `passwordGrantAuthService`

Enable Auth Module Messages for Password Credentials Grant

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.

The Password Grant Type requires the `grant_type=password` parameter.

Default value: `false`

amster attribute: `moduleMessageEnabledInPasswordGrant`

Grant Types

The set of Grant Types (OAuth2 Flows) that are permitted to be used by this client.

If no Grant Types (OAuth2 Flows) are configured nothing will be permitted.

Default value:

```
implicit
urn:ietf:params:oauth:grant-type:saml2-bearer
```

```
refresh_token
password
client_credentials
urn:ietf:params:oauth:grant-type:device_code
authorization_code
urn:openid:params:grant-type:ciba
urn:ietf:params:oauth:grant-type:uma-ticket
urn:ietf:params:oauth:grant-type:token-exchange
urn:ietf:params:oauth:grant-type:jwt-bearer
```

amster attribute: `grantTypes`

Trusted TLS Client Certificate Header

HTTP Header to receive TLS client certificates when TLS is terminated at a proxy.

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.

amster attribute: `tlsClientCertificateTrustedHeader`

TLS Client Certificate Header Format

Format of the HTTP header used to communicate a client certificate from a reverse proxy.

The following formats are supported:

- `URLENCODED_PEM` - a URL-encoded PEM format certificate. This is the format used by Nginx.
- `X_FORWARDED_CLIENT_CERT` - the X-Forwarded-Client-Certformat used by Envoy and Istio.

The possible values for this property are:

- `URLENCODED_PEM`
- `X_FORWARDED_CLIENT_CERT`

Default value: `URLENCODED_PEM`

amster attribute: `tlsClientCertificateHeaderFormat`

Support TLS Certificate-Bound Access Tokens

Whether to bind access tokens to the client certificate when using TLS client certificate authentication.

Default value: `true`

amster attribute: `tlsCertificateBoundAccessTokensEnabled`

Check TLS Certificate Revocation Status

Whether to check if TLS client certificates have been revoked.

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.

Default value: `false`

amster attribute: `tlsCertificateRevocationCheckingEnabled`

OCSP Responder URI

URI of the OCSP responder service to use for checking certificate revocation status.

If specified this value overrides any OCSP or CRL mechanisms specified in individual certificates.

amster attribute: `tlsOcspResponderUri`

OCSP Responder Certificate

PEM-encoded certificate to use to verify OCSP responses.

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.

amster attribute: `tlsOcspResponderCert`

Macaroon Token Format

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.

The possible values for this property are:

- `V1`
- `V2`

Default value: `V2`

amster attribute: `macaroonTokenFormat`

Client Dynamic Registration

The following settings appear on the **Client Dynamic Registration** tab:

Require Software Statement for Dynamic Client Registration

When enabled, a software statement JWT containing at least the `iss` (issuer) claim must be provided when registering an OAuth 2.0 client dynamically.

Default value: `false`

amster attribute: `dynamicClientRegistrationSoftwareStatementRequired`

Required Software Statement Attested Attributes

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.

Leave blank to allow any attributes to be present.

Default value: `redirect_uris`

amster attribute: `requiredSoftwareStatementAttestedAttributes`

Allow Open Dynamic Client Registration

Allow clients to register without an access token. If enabled, you should consider adding some form of rate limiting. For more information, see Client Registration in the OpenID Connect specification.

Default value: `false`

amster attribute: `allowDynamicRegistration`

Generate Registration Access Tokens

Whether to generate Registration Access Tokens for clients that register by using open dynamic client registration. Such tokens allow the client to access the Client Configuration Endpoint as per the OpenID Connect specification. This setting has no effect if Allow Open Dynamic Client Registration is disabled.

Default value: `true`

amster attribute: `generateRegistrationAccessTokens`

Scope to give access to dynamic client registration

Mandatory scope required when registering a new OAuth2 client.

Default value: `dynamic_client_registration`

amster attribute: `dynamicClientRegistrationScope`

OpenID Connect

The following settings appear on the **OpenID Connect** tab:

OIDC Claims Script

The script that is run when issuing an ID token or making a request to the *userinfo* endpoint during OpenID requests.

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.

The possible values for this property are:

- OIDC Claims Script

Default value: `OIDC Claims Script`

amster attribute: `oidcClaimsScript`

Overrideable Id_Token Claims

List of claims in the id_token that may be overrideable in the OIDC Claims Script. These should be the subset of the core OpenID Connect claims, like `aud` or `azp`.

Tip

- For information about the core OpenID Connect claims, see the ID Token data structure.
- For details of the OIDC script, see "Scripting OpenID Connect 1.0 Claims" in the *OpenID Connect 1.0 Guide*.
- To override claims, follow the steps described in How do I override claims in the OIDC ID token in Identity Cloud or AM 7.1.x?

amster attribute: `overrideableOIDCClaims`

ID Token Signing Algorithms supported

Algorithms supported to sign OpenID Connect `id_tokens`.

AM supports signing algorithms listed in JSON Web Algorithms (JWA): "alg" (Algorithm) Header Parameter Values for JWS:

- `HS256` - HMAC with SHA-256.
- `HS384` - HMAC with SHA-384.
- `HS512` - HMAC with SHA-512.
- `ES256` - ECDSA with SHA-256 and NIST standard P-256 elliptic curve.
- `ES384` - ECDSA with SHA-384 and NIST standard P-384 elliptic curve.
- `ES512` - ECDSA with SHA-512 and NIST standard P-521 elliptic curve.
- `RS256` - RSASSA-PKCS-v1_5 using SHA-256.
- `RS384` - RSASSA-PKCS-v1_5 using SHA-384.
- `RS512` - RSASSA-PKCS-v1_5 using SHA-512.

- `PS256` - RSASSA-PSS using SHA-256.
- `PS384` - RSASSA-PSS using SHA-384.
- `PS512` - RSASSA-PSS using SHA-512.

Default value:

```
PS384
ES384
RS384
HS256
HS512
ES256
RS256
HS384
ES512
PS256
PS512
RS512
```

amster attribute: `supportedIDTokenSigningAlgorithms`

ID Token Encryption Algorithms supported

Encryption algorithms supported to encrypt OpenID Connect ID tokens in order to hide its contents.

AM supports the following ID token encryption algorithms:

- `RSA-OAEP` - RSA with Optimal Asymmetric Encryption Padding (OAEP) with SHA-1 and MGF-1.
- `RSA-OAEP-256` - RSA with OAEP with SHA-256 and MGF-1.
- `A128KW` - AES Key Wrapping with 128-bit key derived from the client secret.
- `RSA1_5` - RSA with PKCS#1 v1.5 padding.
- `A256KW` - AES Key Wrapping with 256-bit key derived from the client secret.
- `dir` - Direct encryption with AES using the hashed client secret.
- `A192KW` - AES Key Wrapping with 192-bit key derived from the client secret.

Default value:

```
ECDH-ES+A256KW
ECDH-ES+A192KW
RSA-OAEP
ECDH-ES+A128KW
RSA-OAEP-256
A128KW
A256KW
ECDH-ES
```

```
dir
A192KW
```

amster attribute: `supportedIDTokenEncryptionAlgorithms`

ID Token Encryption Methods supported

Encryption methods supported to encrypt OpenID Connect ID tokens in order to hide its contents.

AM supports the following ID token encryption algorithms:

- `A128GCM`, `A192GCM`, and `A256GCM` - AES in Galois Counter Mode (GCM) authenticated encryption mode.
- `A128CBC-HS256`, `A192CBC-HS384`, and `A256CBC-HS512` - AES encryption in CBC mode, with HMAC-SHA-2 for integrity.

Default value:

```
A256GCM
A192GCM
A128GCM
A128CBC-HS256
A192CBC-HS384
A256CBC-HS512
```

amster attribute: `supportedIDTokenEncryptionMethods`

Supported Claims

Set of claims supported by the OpenID Connect `/oauth2/userinfo` endpoint, with translations.

Claims may be entered as simple strings or pipe separated strings representing the internal claim name, locale, and localized description.

For example: `name|en|Your full name.`.

Locale strings are in the format: `language + "_" + country + "_" + variant`, for example `en`, `en_GB`, or `en_US_WIN`. If the locale and pipe is omitted, the description is displayed to all users that have undefined locales.

If the description is also omitted, nothing is displayed on the consent page for the claim. For example specifying `family_name|` would allow the claim `family_name` to be used by the client, but would not display it to the user on the consent page when requested.

amster attribute: `supportedClaims`

OpenID Connect JWT Token Lifetime (seconds)

The amount of time the JWT will be valid for, in seconds.

Default value: `3600`

amster attribute: `jwtTokenLifetime`

OIDC Provider Discovery

Turns on and off OIDC Discovery endpoint.

Default value: `false`

amster attribute: `oidcDiscoveryEndpointEnabled`

Advanced OpenID Connect

The following settings appear on the **Advanced OpenID Connect** tab:

Remote JSON Web Key URL

The Remote URL where the providers JSON Web Key can be retrieved.

If this setting is not configured, then AM provides a local URL to access the public key of the private key used to sign ID tokens.

amster attribute: `jkwsURI`

Idtokeninfo Endpoint Requires Client Authentication

When enabled, the `/oauth2/idtokeninfo` endpoint requires client authentication if the signing algorithm is set to `HS256`, `HS384`, or `HS512`.

Default value: `true`

amster attribute: `idTokenInfoClientAuthenticationEnabled`

Enable "claims_parameter_supported"

If enabled, clients will be able to request individual claims using the `claims` request parameter, as per section 5.5 of the OpenID Connect specification.

Default value: `false`

amster attribute: `claimsParameterSupported`

OpenID Connect acr_values to Auth Chain Mapping

Maps OpenID Connect ACR values to authentication chains. For more details, see the acr_values parameter in the OpenID Connect authentication request specification.

amster attribute: `loaMapping`

Default ACR values

Default requested Authentication Context Class Reference values.

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.

amster attribute: `defaultACR`

OpenID Connect id_token amr Values to Auth Module Mappings

Specify `amr` values to be returned in the OpenID Connect `id_token`. Once authentication has completed, the authentication modules that were used from the authentication service will be mapped to the `amr` values. If you do not require `amr` values, or are not providing OpenID Connect tokens, leave this field blank.

amster attribute: `amrMappings`

Always Return Claims in ID Tokens

If enabled, include scope-derived claims in the `id_token`, even if an access token is also returned that could provide access to get the claims from the `userinfo` endpoint.

If not enabled, if an access token is requested the client must use it to access the `userinfo` endpoint for scope-derived claims, as they will not be included in the ID token.

Default value: `false`

amster attribute: `alwaysAddClaimsToToken`

Enable Session Management

If this is not enabled then OpenID Connect session management related endpoints will be disabled. When enabled AM will store *ops* tokens corresponding to OpenID Connect sessions in the CTS store and an oidc session id in the AM session.

Default value: `true`

amster attribute: `storeOpsTokens`

Request Parameter Signing Algorithms Supported

Algorithms supported to verify signature of Request parameterAM supports signing algorithms listed in JSON Web Algorithms (JWA): "alg" (Algorithm) Header Parameter Values for JWS:

- `HS256` - HMAC with SHA-256.
- `HS384` - HMAC with SHA-384.
- `HS512` - HMAC with SHA-512.

- `ES256` - ECDSA with SHA-256 and NIST standard P-256 elliptic curve.
- `ES384` - ECDSA with SHA-384 and NIST standard P-384 elliptic curve.
- `ES512` - ECDSA with SHA-512 and NIST standard P-521 elliptic curve.
- `RS256` - RSASSA-PKCS-v1_5 using SHA-256.

Default value:

```
PS384
ES384
RS384
HS256
HS512
ES256
RS256
HS384
ES512
PS256
PS512
RS512
```

amster attribute: `supportedRequestParameterSigningAlgorithms`

Request Parameter Encryption Algorithms Supported

Encryption algorithms supported to decrypt Request parameter.

AM supports the following ID token encryption algorithms:

- `RSA-OAEP` - RSA with Optimal Asymmetric Encryption Padding (OAEP) with SHA-1 and MGF-1.
- `RSA-OAEP-256` - RSA with OAEP with SHA-256 and MGF-1.
- `A128KW` - AES Key Wrapping with 128-bit key derived from the client secret.
- `RSA1_5` - RSA with PKCS#1 v1.5 padding.
- `A256KW` - AES Key Wrapping with 256-bit key derived from the client secret.
- `dir` - Direct encryption with AES using the hashed client secret.
- `A192KW` - AES Key Wrapping with 192-bit key derived from the client secret.

Default value:

```
ECDH-ES+A256KW
ECDH-ES+A192KW
ECDH-ES+A128KW
RSA-OAEP
RSA-OAEP-256
A128KW
A256KW
```

```
ECDH-ES
dir
A192KW
```

amster attribute: `supportedRequestParameterEncryptionAlgorithms`

Request Parameter Encryption Methods Supported

Encryption methods supported to decrypt Request parameter.

AM supports the following Request parameter encryption algorithms:

- `A128GCM`, `A192GCM`, and `A256GCM` - AES in Galois Counter Mode (GCM) authenticated encryption mode.
- `A128CBC-HS256`, `A192CBC-HS384`, and `A256CBC-HS512` - AES encryption in CBC mode, with HMAC-SHA-2 for integrity.

Default value:

```
A256GCM
A192GCM
A128GCM
A128CBC-HS256
A192CBC-HS384
A256CBC-HS512
```

amster attribute: `supportedRequestParameterEncryptionEnc`

Supported Token Endpoint JWS Signing Algorithms.

Supported JWS Signing Algorithms for 'private_key_jwt' JWT based authentication method.

Default value:

```
PS384
ES384
RS384
HS256
HS512
ES256
RS256
HS384
ES512
PS256
PS512
RS512
```

amster attribute: `supportedTokenEndpointAuthenticationSigningAlgorithms`

Authorized OIDC SSO Clients

Clients authorized to use OpenID Connect ID tokens as SSO Tokens.

Allows clients to act with the full authority of the user. Grant this permission only to trusted clients.

amster attribute: `authorisedOpenIdConnectSSOClients`

UserInfo Signing Algorithms Supported

Algorithms supported to verify signature of the UserInfo endpoint. AM supports signing algorithms listed in JSON Web Algorithms (JWA): "alg" (Algorithm) Header Parameter Values for JWS:

- `HS256` - HMAC with SHA-256.
- `HS384` - HMAC with SHA-384.
- `HS512` - HMAC with SHA-512.
- `ES256` - ECDSA with SHA-256 and NIST standard P-256 elliptic curve.
- `ES384` - ECDSA with SHA-384 and NIST standard P-384 elliptic curve.
- `ES512` - ECDSA with SHA-512 and NIST standard P-521 elliptic curve.
- `RS256` - RSASSA-PKCS-v1_5 using SHA-256.

Default value:

```
ES384
HS256
HS512
ES256
RS256
HS384
ES512
```

amster attribute: `supportedUserInfoSigningAlgorithms`

UserInfo Encryption Algorithms Supported

Encryption algorithms supported by the UserInfo endpoint.

AM supports the following UserInfo endpoint encryption algorithms:

- `RSA-OAEP` - RSA with Optimal Asymmetric Encryption Padding (OAEP) with SHA-1 and MGF-1.
- `RSA-OAEP-256` - RSA with OAEP with SHA-256 and MGF-1.
- `A128KW` - AES Key Wrapping with 128-bit key derived from the client secret.
- `RSA1_5` - RSA with PKCS#1 v1.5 padding.
- `A256KW` - AES Key Wrapping with 256-bit key derived from the client secret.

- `dir` - Direct encryption with AES using the hashed client secret.
- `A192KW` - AES Key Wrapping with 192-bit key derived from the client secret.

Default value:

```
ECDH-ES+A256KW
ECDH-ES+A192KW
RSA-OAEP
ECDH-ES+A128KW
RSA-OAEP-256
A128KW
A256KW
ECDH-ES
dir
A192KW
```

amster attribute: `supportedUserInfoEncryptionAlgorithms`

UserInfo Encryption Methods Supported

Encryption methods supported by the UserInfo endpoint.

AM supports the following UserInfo endpoint encryption methods:

- `A128GCM`, `A192GCM`, and `A256GCM` - AES in Galois Counter Mode (GCM) authenticated encryption mode.
- `A128CBC-HS256`, `A192CBC-HS384`, and `A256CBC-HS512` - AES encryption in CBC mode, with HMAC-SHA-2 for integrity.

Default value:

```
A256GCM
A192GCM
A128GCM
A128CBC-HS256
A192CBC-HS384
A256CBC-HS512
```

amster attribute: `supportedUserInfoEncryptionEnc`

Use Force Authentication for `prompt=login`

This setting is applied only when you've implemented modules or chains, and you've specified the `prompt=login` parameter. The default value is `false`.

When set to `false`, AM forces the end user to authenticate even if they already have a valid session. After re-authentication, AM creates a new session.

When set to `true`, AM forces the end user to authenticate even if they already have a valid session. But, after re-authentication, AM returns the same session ID.

Caution

If you set `Use Force Authentication for prompt=login` to `true`, you *must also* set the `org.forgerock.openam.authentication.forceAuth.enabled` advanced server property to `true`. If you do not do this, your users may end up in an infinite login loop.

For security reasons, it is strongly recommended that you leave `Use Force Authentication for prompt=login` set to the default value (`false`), so that a new session is created when the user re-authenticates.

Token Introspection Response Signing Algorithms Supported

Algorithms that are supported for signing the Token Introspection endpoint JWT response.

AM supports signing algorithms listed in JSON Web Algorithms (JWA): "alg" (Algorithm) Header Parameter Values for JWS:

- `HS256` - HMAC with SHA-256.
- `HS384` - HMAC with SHA-384.
- `HS512` - HMAC with SHA-512.
- `ES256` - ECDSA with SHA-256 and NIST standard P-256 elliptic curve.
- `ES384` - ECDSA with SHA-384 and NIST standard P-384 elliptic curve.
- `ES512` - ECDSA with SHA-512 and NIST standard P-521 elliptic curve.
- `RS256` - RSASSA-PKCS-v1_5 using SHA-256.
- `RS384` - RSASSA-PKCS-v1_5 using SHA-384.
- `RS512` - RSASSA-PKCS-v1_5 using SHA-512.
- `EdDSA` - EdDSA with SHA-512.

Default value:

```
PS384
RS384
EdDSA
ES384
HS256
HS512
ES256
RS256
HS384
ES512
PS256
PS512
RS512
```

amster attribute: `supportedTokenIntrospectionResponseSigningAlgorithms`

Token Introspection Response Encryption Algorithms Supported

Encryption algorithms supported by the Token Introspection endpoint JWT response.

AM supports the following UserInfo endpoint encryption algorithms:

- `RSA-OAEP` - RSA with Optimal Asymmetric Encryption Padding (OAEP) with SHA-1 and MGF-1.
- `RSA-OAEP-256` - RSA with OAEP with SHA-256 and MGF-1.
- `A128KW` - AES Key Wrapping with 128-bit key derived from the client secret.
- `RSA1_5` - RSA with PKCS#1 v1.5 padding.
- `A256KW` - AES Key Wrapping with 256-bit key derived from the client secret.
- `dir` - Direct encryption with AES using the hashed client secret.
- `A192KW` - AES Key Wrapping with 192-bit key derived from the client secret.

Default value:

```
ECDH-ES+A256KW
ECDH-ES+A192KW
RSA-OAEP
ECDH-ES+A128KW
RSA-OAEP-256
A128KW
A256KW
ECDH-ES
dir
A192KW
```

amster attribute: `supportedTokenIntrospectionResponseEncryptionAlgorithms`

Token Introspection Response Encryption Methods Supported

Encryption methods supported by the Token Introspection endpoint JWT response.

AM supports the following encryption methods:

- `A128GCM`, `A192GCM`, and `A256GCM` - AES in Galois Counter Mode (GCM) authenticated encryption mode.
- `A128CBC-HS256`, `A192CBC-HS384`, and `A256CBC-HS512` - AES encryption in CBC mode, with HMAC-SHA-2 for integrity.

Default value:

```
A256GCM
```

```
A192GCM
A128GCM
A128CBC-HS256
A192CBC-HS384
A256CBC-HS512
```

amster attribute: `supportedTokenIntrospectionResponseEncryptionEnc`

Include all kty and alg combinations in jwks_uri

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. RFC7517 distinct key KIDs

Default value: `false`

amster attribute: `includeAllKtyAlgCombinationsInJwksUri`

Device Flow

The following settings appear on the **Device Flow** tab:

Verification URL

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.

amster attribute: `verificationUrl`

Device Completion URL

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.

amster attribute: `completionUrl`

Device Code Lifetime (seconds)

The lifetime of the device code, in seconds.

Default value: `300`

amster attribute: `deviceCodeLifetime`

Device Polling Interval

The polling frequency for devices waiting for tokens when using the device code flow.

Default value: `5`

amster attribute: `devicePollInterval`

Consent

The following settings appear on the **Consent** tab:

Saved Consent Attribute Name

Name of a multi-valued attribute on resource owner profiles where AM can save authorization consent decisions.

When the resource owner chooses to save the decision to authorize access for a client application, then AM updates the resource owner's profile to avoid having to prompt the resource owner to grant authorization when the client issues subsequent authorization requests.

amster attribute: `savedConsentAttribute`

Allow Clients to Skip Consent

If enabled, clients may be configured so that the resource owner will not be asked for consent during authorization flows.

Default value: `false`

amster attribute: `clientsCanSkipConsent`

Enable Remote Consent

Enables consent to be gathered by a separate service.

Default value: `false`

amster attribute: `enableRemoteConsent`

Remote Consent Service ID

The ID of an existing remote consent service agent.

The possible values for this property are:

- `[Empty]`

amster attribute: `remoteConsentServiceId`

Remote Consent Service Request Signing Algorithms Supported

Algorithms supported to sign consent_request JWTs for Remote Consent Services.

AM supports signing algorithms listed in JSON Web Algorithms (JWA): "alg" (Algorithm) Header Parameter Values for JWS:

- `HS256` - HMAC with SHA-256.

- `HS384` - HMAC with SHA-384.
- `HS512` - HMAC with SHA-512.
- `ES256` - ECDSA with SHA-256 and NIST standard P-256 elliptic curve.
- `ES384` - ECDSA with SHA-384 and NIST standard P-384 elliptic curve.
- `ES512` - ECDSA with SHA-512 and NIST standard P-521 elliptic curve.
- `RS256` - RSASSA-PKCS-v1_5 using SHA-256.

Default value:

```
PS384
ES384
RS384
HS256
HS512
ES256
RS256
HS384
ES512
PS256
PS512
RS512
```

amster attribute: `supportedRcsRequestSigningAlgorithms`

Remote Consent Service Request Encryption Algorithms Supported

Encryption algorithms supported to encrypt Remote Consent Service requests.

AM supports the following encryption algorithms:

- `RSA1_5` - RSA with PKCS#1 v1.5 padding.
- `RSA-OAEP` - RSA with Optimal Asymmetric Encryption Padding (OAEP) with SHA-1 and MGF-1.
- `RSA-OAEP-256` - RSA with OAEP with SHA-256 and MGF-1.
- `A128KW` - AES Key Wrapping with 128-bit key derived from the client secret.
- `A192KW` - AES Key Wrapping with 192-bit key derived from the client secret.
- `A256KW` - AES Key Wrapping with 256-bit key derived from the client secret.
- `dir` - Direct encryption with AES using the hashed client secret.

Default value:

```
ECDH-ES+A256KW
ECDH-ES+A192KW
```

```
RSA-OAEP
ECDH-ES+A128KW
RSA-OAEP-256
A128KW
A256KW
ECDH-ES
dir
A192KW
```

amster attribute: `supportedRcsRequestEncryptionAlgorithms`

Remote Consent Service Request Encryption Methods Supported

Encryption methods supported to encrypt Remote Consent Service requests.

AM supports the following encryption methods:

- `A128GCM`, `A192GCM`, and `A256GCM` - AES in Galois Counter Mode (GCM) authenticated encryption mode.
- `A128CBC-HS256`, `A192CBC-HS384`, and `A256CBC-HS512` - AES encryption in CBC mode, with HMAC-SHA-2 for integrity.

Default value:

```
A256GCM
A192GCM
A128GCM
A128CBC-HS256
A192CBC-HS384
A256CBC-HS512
```

amster attribute: `supportedRcsRequestEncryptionMethods`

Remote Consent Service Response Signing Algorithms Supported

Algorithms supported to verify signed consent_response JWT from Remote Consent Services.

AM supports signing algorithms listed in JSON Web Algorithms (JWA): "alg" (Algorithm) Header Parameter Values for JWS:

- `HS256` - HMAC with SHA-256.
- `HS384` - HMAC with SHA-384.
- `HS512` - HMAC with SHA-512.
- `ES256` - ECDSA with SHA-256 and NIST standard P-256 elliptic curve.
- `ES384` - ECDSA with SHA-384 and NIST standard P-384 elliptic curve.
- `ES512` - ECDSA with SHA-512 and NIST standard P-521 elliptic curve.

- `RS256` - RSASSA-PKCS-v1_5 using SHA-256.

Default value:

```
PS384
ES384
RS384
HS256
HS512
ES256
RS256
HS384
ES512
PS256
PS512
RS512
```

amster attribute: `supportedRcsResponseSigningAlgorithms`

Remote Consent Service Response Encryption Algorithms Supported

Encryption algorithms supported to decrypt Remote Consent Service responses.

AM supports the following encryption algorithms:

- `RSA1_5` - RSA with PKCS#1 v1.5 padding.
- `RSA-OAEP` - RSA with Optimal Asymmetric Encryption Padding (OAEP) with SHA-1 and MGF-1.
- `RSA-OAEP-256` - RSA with OAEP with SHA-256 and MGF-1.
- `A128KW` - AES Key Wrapping with 128-bit key derived from the client secret.
- `A192KW` - AES Key Wrapping with 192-bit key derived from the client secret.
- `A256KW` - AES Key Wrapping with 256-bit key derived from the client secret.
- `dir` - Direct encryption with AES using the hashed client secret.

Default value:

```
ECDH-ES+A256KW
ECDH-ES+A192KW
ECDH-ES+A128KW
RSA-OAEP
RSA-OAEP-256
A128KW
A256KW
ECDH-ES
dir
A192KW
```

amster attribute: `supportedRcsResponseEncryptionAlgorithms`

Remote Consent Service Response Encryption Methods Supported

Encryption methods supported to decrypt Remote Consent Service responses.

AM supports the following encryption methods:

- `A128GCM`, `A192GCM`, and `A256GCM` - AES in Galois Counter Mode (GCM) authenticated encryption mode.
- `A128CBC-HS256`, `A192CBC-HS384`, and `A256CBC-HS512` - AES encryption in CBC mode, with HMAC-SHA-2 for integrity.

Default value:

```
A256GCM
A192GCM
A128GCM
A128CBC-HS256
A192CBC-HS384
A256CBC-HS512
```

amster attribute: `supportedRcsResponseEncryptionMethods`

CIBA

The following settings appear on the **CIBA** tab:

Back Channel Authentication ID Lifetime (seconds)

The time back channel authentication request id is valid for, in seconds.

Default value: `600`

amster attribute: `cibaAuthReqIdLifetime`

Polling Wait Interval (seconds)

The minimum amount of time in seconds that the Client should wait between polling requests to the token endpoint

Default value: `2`

amster attribute: `cibaMinimumPollingInterval`

Signing Algorithms Supported

Algorithms supported to sign the CIBA request parameter.

AM supports signing algorithms listed in JSON Web Algorithms (JWA): "alg" (Algorithm) Header Parameter Values for JWS:

- `ES256` - ECDSA with SHA-256 and NIST standard P-256 elliptic curve.
- `PS256` - RSASSA-PSS using SHA-256.

Default value:

```
ES256
PS256
```

amster attribute: `supportedCibaSigningAlgorithms`

Platform

amster service name: `Platform`

The following settings are available in this service:

Platform Locale

Set the fallback locale used when the user locale cannot be determined.

Default value: `en_US`

amster attribute: `locale`

Cookie Domains

Set the list of domains into which AM writes cookies.

If you set multiple cookie domains, AM only sets the cookie in the domain the client uses to access AM.

If you do not set a value here, the `Set-Cookie` response header will not include a `Domain` attribute. In this case, AM sets a host-only cookie rather than a domain cookie.

Because host-only cookies are more secure than domain cookies, you *should* use host-only cookies unless you have a good business case for using domain cookies. In general, domain cookies are required only if your Web or Java agent uses an SSO tracking cookie for SSO.

Default value: `openam.example.com`

amster attribute: `cookieDomains`

Policy Configuration

amster service name: `PolicyConfiguration`

Global Attributes

The following settings appear on the **Global Attributes** tab:

Resource Comparator

AM uses resource comparators to match resources specified in policy rules. When setting comparators on the command line, separate fields with `|` characters.

Default value: `serviceType=iPlanetAMWebAgentService|class=com.sun.identity.policy.plugins.HttpURLResourceName|wildcard=*|oneLevelWildcard=-*-|delimiter=/|caseSensitive=false`

amster attribute: `resourceComparators`

Continue Evaluation on Deny Decision

If no, then AM stops evaluating policy as soon as it reaches a deny decision.

Default value: `false`

amster attribute: `continueEvaluationOnDeny`

Realm Alias Referrals

If yes, then AM allows creation of policies for HTTP and HTTPS resources whose FQDN matches the DNS alias for the realm even when no referral policy exists.

Default value: `false`

amster attribute: `realmAliasReferrals`

Realm Defaults

The following settings appear on the **Realm Defaults** tab:

Primary LDAP Server

Configuration directory server host:port that AM searches for policy information.

Format: `local AM server name | hostname:port`

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.

For example, openam.example.com|opendj.example.com:1389 opendj.example.com:2389

Default value: `openam.example.com:50636`

amster attribute: `ldapServer`

LDAP Users Base DN

Base DN for LDAP Users subject searches.

Default value: `dc=openam,dc=forgerock,dc=org`

amster attribute: `usersBaseDn`

LDAP Bind DN

Bind DN to connect to the directory server for policy information.

Default value: `cn=Directory Manager`

amster attribute: `bindDn`

LDAP Bind Password

Bind password to connect to the directory server for policy information.

amster attribute: `bindPassword`

LDAP Organization Search Filter

Search filter to match organization entries.

Default value: `(objectclass=sunismanagedorganization)`

amster attribute: `realmSearchFilter`

LDAP Users Search Filter

Search filter to match user entries.

Default value: `(objectclass=inetorgperson)`

amster attribute: `usersSearchFilter`

LDAP Users Search Scope

Search scope to find user entries.

The possible values for this property are:

- `SCOPE_BASE`
- `SCOPE_ONE`
- `SCOPE_SUB`

Default value: `SCOPE_SUB`

amster attribute: `usersSearchScope`

LDAP Users Search Attribute

Naming attribute for user entries.

Default value: `uid`

amster attribute: `usersSearchAttribute`

Maximum Results Returned from Search

Search limit for LDAP searches.

Default value: `100`

amster attribute: `maximumSearchResults`

Search Timeout

Time after which AM returns an error for an incomplete search, in seconds.

Default value: `5`

amster attribute: `searchTimeout`

LDAP SSL/TLS

If enabled, AM connects securely to the directory server. This requires that you install the directory server certificate.

Default value: `true`

amster attribute: `sslEnabled`

LDAP Connection Pool Minimum Size

Minimum number of connections in the pool.

Default value: `1`

amster attribute: `connectionPoolMinimumSize`

LDAP Connection Pool Maximum Size

Maximum number of connections in the pool.

Default value: `10`

amster attribute: `connectionPoolMaximumSize`

Heartbeat Interval

Specifies how often should AM send a heartbeat request to the directory.

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.

Default value: `10`

amster attribute: `policyHeartbeatInterval`

Heartbeat Unit

Defines the time unit corresponding to the Heartbeat Interval setting.

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.

The possible values for this property are:

- Label: **second** (Value: `SECONDS`)
- Label: **minute** (Value: `MINUTES`)
- Label: **hour** (Value: `HOURS`)

Default value: `SECONDS`

amster attribute: `policyHeartbeatTimeUnit`

Subjects Result Time to Live

Maximum time that AM caches a subject result for evaluating policy requests, in minutes. A value of `0` prevents AM from caching subject evaluations for policy decisions.

Default value: `10`

amster attribute: `subjectsResultTTL`

User Alias

If enabled, AM can evaluate policy for remote users aliased to local users.

Default value: `false`

amster attribute: `userAliasEnabled`

Check resources exist when Resource Server is updated

Check all registered resources exist when updating Resource Server.

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.

Default value: `true`

amster attribute: `checkIfResourceTypeExists`

Push Notification Service

amster service name: `PushNotification`

Realm Defaults

The following settings appear on the **Realm Defaults** tab:

SNS Access Key ID

Amazon Simple Notification Service Access Key ID. For more information, see https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_access-keys.html.

For example, you might set this property to: *AKIAIOSFODNN7EXAMPLE*

amster attribute: `accessKey`

SNS Access Key Secret

Amazon Simple Notification Service Access Key Secret. For more information, see https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_access-keys.html.

amster attribute: `secret`

SNS Endpoint for APNS

The Simple Notification Service endpoint in Amazon Resource Name format, used to send push messages to the Apple Push Notification Service (APNS).

For example, you might set this property to: *arn:aws:sns:us-east-1:1234567890:app/APNS/production*

amster attribute: `appleEndpoint`

SNS Endpoint for GCM

The Simple Notification Service endpoint in Amazon Resource Name format, used to send push messages over Google Cloud Messaging (GCM).

For example, you might set this property to: *arn:aws:sns:us-east-1:1234567890:app/GCM/production*

amster attribute: `googleEndpoint`

SNS Client Region

Region of your registered Amazon Simple Notification Service client. For more information, see https://docs.aws.amazon.com/general/latest/gr/rande.html.

The possible values for this property are:

- `us-gov-west-1`
- `us-east-1`
- `us-west-1`
- `us-west-2`
- `eu-west-1`
- `eu-central-1`
- `ap-southeast-1`
- `ap-southeast-2`
- `ap-northeast-1`
- `ap-northeast-2`
- `sa-east-1`
- `n-north-1`

Default value: `us-east-1`

amster attribute: `region`

Message Transport Delegate Factory

The fully qualified class name of the factory responsible for creating the PushNotificationDelegate. The class must implement `org.forgerock.openam.services.push.PushNotificationDelegate`.

Default value: `org.forgerock.openam.services.push.sns.SnsHttpDelegateFactory`

amster attribute: `delegateFactory`

Response Cache Duration

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 `0`.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.

Default value: `120`

amster attribute: `mdDuration`

Response Cache Concurrency

Level of concurrency to use when accessing the message dispatcher cache. Defaults to `16`, and must be greater than `0`. Choose a value to accommodate as many threads as will ever concurrently access the message dispatcher cache.

Default value: `16`

amster attribute: `mdConcurrency`

Response Cache Size

Maximum size of the message dispatcher cache, in number of records. If set to `0` 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.

Default value: `10000`

amster attribute: `mdCacheSize`

RADIUS Server

amster service name: `RadiusServer`

Configuration

The following settings appear on the **Configuration** tab:

Enabled

Enables the AM RADIUS server to listen for requests on the listener port and to handle the requests.

The possible values for this property are:

- `NO`
- `YES`

Default value: `NO`

amster attribute: `radiusListenerEnabled`

Listener Port

The UDP port on which each AM server will listen for RADIUS Access-Request packets

According to the RADIUS Authentication Specification, RFC 2865, the officially assigned port number for RADIUS is `1812`. Specify a value from `1024` to `65535`. All client requests are handled through the same port.

Default value: `1812`

amster attribute: `radiusServerPort`

Thread Pool Core Size

When a RADIUS request is received and fewer than `corePoolSize` 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 `1` to `100`.

Default value: `1`

amster attribute: `radiusThreadPoolCoreSize`

Thread Pool Max Size

Maximum number of threads allowed in the pool. See also "Thread Pool Core Size".

Default value: `10`

amster attribute: `radiusThreadPoolMaxSize`

Thread Pool Keep-Alive Seconds

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 `1` to `3600`.

Default value: `10`

amster attribute: `radiusThreadPoolKeepaliveSeconds`

Thread Pool Queue Size

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 `1` to `1000`.

Default value: `20`

amster attribute: `radiusThreadPoolQueueSize`

Secondary Configurations

This service has the following Secondary Configurations.

radiusClient

Client IP Address

The IP Address of the client.

Section 5.4 of the RADIUS Authentication Specification, RFC 2865, indicates that the source IP address of the Access-Request packet *MUST* be used to identify a configured client and hence determine the shared secret to use for decrypting the User-Password field.

This property should hold the source IP address of the client. This should match the value obtained from Java's `InetSocketAddress.getAddress().toString()` function.

To verify the value, send an Access-Request packet to AM's RADIUS port and watch for a message stating: `"No Defined RADIUS Client matches IP address '/127.0.0.1'. Dropping request."`. The value used in this property should match the IP address returned in the single quotes.

Default value: `/127.0.0.1`

amster attribute: `clientIpAddress`

Client Secret

This secret shared between server and client for encryption of the user password.

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.

amster attribute: `clientSecret`

Log Packet Contents for this Client

Indicates if full packet contents should be dumped to the log.

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.

Default value: `NO`

amster attribute: `clientPacketsLogged`

Handler Class

The fully qualified name of a class to handle incoming RADIUS Access-Requests for this client.

This class must implement the `com.sun.identity.authentication.modules.radius.server.spi.AccessRequestHandler` 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.

Default value: `org.forgerock.openam.radius.server.spi.handlers.OpenAMAuthHandler`

amster attribute: `handlerClass`

Handler Class Configuration Properties

Properties needed by the handler class for its configuration.

These properties are provided to the handler via its `init` 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 '`=`' character incurred separates a key from its value. All entries are placed in a properties file handed to each handler instance.

Default value:

```
realm=/
chain=ldapService
```

amster attribute: `handlerConfig`

REST APIs

amster service name: `RestApis`

The following settings are available in this service:

Default Resource Version

The API resource version to use when the REST request does not specify an explicit version. Choose from:

- `Latest`. If an explicit version is not specified, the latest resource version of an API is used.
- `Oldest`. 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 *supported* version may not be the first version.

- `None`. If an explicit version is not specified, the request will not be handled and an error status is returned.

The possible values for this property are:

- `Latest`
- `Oldest`
- `None`

Default value: `Latest`

amster attribute: `defaultVersion`

Warning Header

Whether to include a warning header in the response to a request which fails to include the `Accept-API-Version` header.

Default value: `true`

amster attribute: `warningHeader`

API Descriptions

Whether API Explorer and API Docs are enabled in AM 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 AM was built. Note that dynamic documentation generation may not work in some application containers.

The possible values for this property are:

- Label: **Enabled with Dynamic Documentation** (Value: `DYNAMIC`)
- Label: **Enabled with Static Documentation** (Value: `STATIC`)
- `DISABLED`

Default value: `STATIC`

amster attribute: `descriptionsState`

Default Protocol Version

The API protocol version to use when a REST request does not specify an explicit version. Choose from:

- `Oldest`. If an explicit version is not specified, the oldest protocol version is used.
- `Latest`. If an explicit version is not specified, the latest protocol version is used.

- `None`. If an explicit version is not specified, the request will not be handled and an error status is returned.

The possible values for this property are:

- `Latest`
- `Oldest`
- `None`

Default value: `Latest`

amster attribute: `defaultProtocolVersion`

Enable CSRF Protection

If enabled, all non-read/query requests will require the X-Requested-With header to be present.

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.

Default value: `true`

amster attribute: `csrfFilterEnabled`

Remote Consent Service

amster service name: `RemoteConsentService`

Realm Defaults

The following settings appear on the **Realm Defaults** tab:

Client Name

The name used to identify this OAuth 2.0 remote consent service when referencedin other services.

amster attribute: `clientId`

Authorization Server jwk_uri

The jwk_uri for retrieving the authorization server signing and encryption keys.

amster attribute: `jwksUriAS`

JWK Store Cache Timeout (in minutes)

The cache timeout for the JWK store of the authorization server, in minutes.

Default value: `60`

amster attribute: `jwkStoreCacheTimeout`

JWK Store Cache Miss Cache Time (in minutes)

The length of time a cache miss is cached, in minutes.

Default value: `1`

amster attribute: `jwkStoreCacheMissCacheTime`

Consent Response Time Limit (in minutes)

The time limit set on the consent response JWT before it expires, in minutes.

Default value: `2`

amster attribute: `consentResponseTimeLimit`

SAML v2.0 SOAP Binding

amster service name: `SamlV2SoapBinding`

The following settings are available in this service:

Request Handler List

List of handlers to deal with SAML v2.0 requests bound to SOAP.

The required format is: `key=`*`Meta Alias`*`|class=`*`Handler Class`*

Set the *key* property for a request handler to the meta alias, and the *class* property to the name of the class that implements the handler.

For example: `key=/pdp|class=com.sun.identity.xacml.plugins.XACMLAuthzDecisionQueryHandler`

amster attribute: `requestHandlers`

SAML v2.0 Service Configuration

amster service name: `SamlV2ServiceConfiguration`

The following settings are available in this service:

Cache cleanup interval (in seconds)

Time between cache cleanup operations, in seconds.

Default value: `600`

amster attribute: `cacheCleanupInterval`

Attribute name for Name ID information

User entry attribute to store name identifier information.

Default value: `sun-fm-saml2-nameid-info`

amster attribute: `nameIDInfoAttribute`

Attribute name for Name ID information key

User entry attribute to store the name identifier key.

Default value: `sun-fm-saml2-nameid-infokey`

amster attribute: `nameIDInfoKeyAttribute`

Cookie domain for IdP Discovery Service

Specifies the cookie domain for the IDP discovery service.

Default value: `openam.example.com`

amster attribute: `idpDiscoveryCookieDomain`

Cookie type for IdP Discovery Service

Specifies the cookie type to use.

The possible values for this property are:

- `PERSISTENT`
- `SESSION`

Default value: `PERSISTENT`

amster attribute: `idpDiscoveryCookieType`

URL scheme for IdP Discovery Service

Specifies the URL scheme to use.

The possible values for this property are:

- `HTTP`
- `HTTPS`

Default value: `HTTPS`

amster attribute: `idpDiscoveryUrlSchema`

XML Encryption SPI implementation class

Used by the SAML2 engine to *encrypt* and *decrypt* documents.

Default value: `com.sun.identity.saml2.xmlenc.FMEncProvider`

amster attribute: `xmlEncryptionClass`

Include xenc:EncryptedKey inside ds:KeyInfo Element

Specify whether to include the `xenc:EncryptedKey` property inside the `ds:KeyInfo` element.

Default value: `true`

amster attribute: `encryptedKeyInKeyInfo`

XML Signing SPI implementation class

Used by the SAML2 engine to *sign* documents.

Default value: `com.sun.identity.saml2.xmlsig.FMSigProvider`

amster attribute: `xmlSigningClass`

XML Signing Certificate Validation

If enabled, then validate certificates used to sign documents.

Default value: `false`

amster attribute: `signingCertValidation`

CA Certificate Validation

If enabled, then validate CA certificates.

Default value: `false`

amster attribute: `caCertValidation`

Buffer length (in bytes) to decompress request

Specify the size of the buffer used for decompressing requests, in bytes.

Default value: `2048`

amster attribute: `bufferLength`

Scripting

amster service name: `Scripting`

Configuration

The following settings appear on the **Configuration** tab:

Default Script Type

The default script context type when creating a new script.

The possible values for this property are:

- Label: **Policy Condition** (Value: `POLICY_CONDITION`)
- Label: **Server-side Authentication** (Value: `AUTHENTICATION_SERVER_SIDE`)
- Label: **Client-side Authentication** (Value: `AUTHENTICATION_CLIENT_SIDE`)
- Label: **OIDC Claims** (Value: `OIDC_CLAIMS`)
- Label: **Decision node script for authentication trees** (Value: `AUTHENTICATION_TREE_DECISION_NODE`)
- Label: **OAuth2 Access Token Modification** (Value: `OAUTH2_ACCESS_TOKEN_MODIFICATION`)
- Label: **Social Identity Provider Profile Transformation** (Value: `SOCIAL_IDP_PROFILE_TRANSFORMATION`)
- Label: **OAuth2 May Act** (Value: `OAUTH2_MAY_ACT`)

Default value: `POLICY_CONDITION`

amster attribute: `defaultContext`

Secondary Configurations

This service has the following Secondary Configurations.

Engine Configuration

The following properties are available for Scripting Service secondary configuration instances:

Engine Configuration

Configure script engine parameters for running a particular script type in AM.

ssoadm attribute: `engineConfiguration`

To access a secondary configuration instance using the **ssoadm** command, use: `--subconfigname [primary configuration]/[secondary configuration]` For example:

```
$ ssoadm set-sub-cfg \
  --adminid uid=amAdmin,ou=People,dc=openam,dc=forgerock,dc=org \
  --password-file admin_pwd_file \
  --servicename ScriptingService \
  --subconfigname OIDC_CLAIMS/engineConfiguration \
  --operation set \
  --attributevalues maxThreads=300 queueSize=-1
```

Note

Supports server-side scripts only. AM cannot configure engine settings for client-side scripts.

The configurable engine settings are as follows:

Server-side Script Timeout

The maximum execution time any individual script should take on the server (in seconds). AM terminates scripts which take longer to run than this value.

ssoadm attribute: `serverTimeout`

Core thread pool size

The initial number of threads in the thread pool from which scripts operate. AM will ensure the pool contains at least this many threads.

ssoadm attribute: `coreThreads`

Maximum thread pool size

The maximum number of threads in the thread pool from which scripts operate. If no free thread is available in the pool, AM creates new threads in the pool for script execution up to the configured maximum. It is recommended to set the maximum number of threads to 300.

ssoadm attribute: `maxThreads`

Thread pool queue size

Specifies the number of threads to use for buffering script execution requests when the maximum thread pool size is reached.

For short, CPU-bound scripts, consider a small pool size and larger queue length. For I/O-bound scripts, for example, REST calls, consider a larger maximum pool size and a smaller queue.

Not hot-swappable: restart server for changes to take effect.

ssoadm attribute: `queueSize`

Thread idle timeout (seconds)

Length of time (in seconds) for a thread to be idle before AM terminates created threads. If the current pool size contains the number of threads set in `Core thread pool size` idle threads will not be terminated, to maintain the initial pool size.

ssoadm attribute: `idleTimeout`

Java class whitelist

Specifies the list of class-name patterns allowed to be invoked by the script. Every class accessed by the script must match at least one of these patterns.

You can specify the class name as-is or use a regular expression.

ssoadm attribute: `whiteList`

Java class blacklist

Specifies the list of class-name patterns that are NOT allowed to be invoked by the script. The blacklist is applied AFTER the whitelist to exclude those classes - access to a class specified in both the whitelist and the blacklist will be denied.

You can specify the class name to exclude as-is or use a regular expression.

ssoadm attribute: `blackList`

Use system SecurityManager

If enabled, AM will make a call to `System.getSecurityManager().checkPackageAccess(...)` for each class that is accessed. The method throws `SecurityException` if the calling thread is not allowed to access the package.

> **Note**
>
> This feature only takes effect if the security manager is enabled for the JVM.

ssoadm attribute: `useSecurityManager`

Scripting languages

Select the languages available for scripts on the chosen type. Either `GROOVY` or `JAVASCRIPT`.

ssoadm attribute: `languages`

Default Script

The source code that is presented as the default when creating a new script of this type.

ssoadm attribute: `defaultScript`

Session

amster service name: `SessionUserService`

General

The following settings appear on the **General** tab:

Latest Access Time Update Frequency

Defaults to `60` seconds. At most, AM updates a session's latest access time this often.

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.

Refreshing a session returns the idle time as the number of seconds since an update has occurred, which will be between `0` and the specified Latest Access Time Update Frequency.

Default value: `60`

amster attribute: `latestAccessTimeUpdateFrequency`

DN Restriction Only Enabled

If enabled, AM will not perform DNS lookups when checking restrictions in cookie hijacking mode.

Default value: `false`

amster attribute: `dnRestrictionOnly`

Session Timeout Handler implementations

Lists plugin classes implementing session timeout handlers. Specify the fully qualified name.

amster attribute: `timeoutHandlers`

Session Search

The following settings appear on the **Session Search** tab:

Maximum Number of Search Results

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.

Default value: `120`

amster attribute: `maxSessionListSize`

Timeout for Search

Time after which AM sees an incomplete search as having failed, in seconds.

Default value: `5`

amster attribute: `sessionListRetrievalTimeout`

Session Property Change Notifications

The following settings appear on the **Session Property Change Notifications** tab:

Enable Property Change Notifications

If on, then AM notifies other applications participating in SSO when a session property in the Notification Properties list changes on a CTS-based session.

The possible values for this property are:

- `ON`
- `OFF`

Default value: `OFF`

amster attribute: `propertyChangeNotifications`

Notification Properties

Lists session properties for which AM can send notifications upon modification. Session notification applies to CTS-based sessions only.

amster attribute: `notificationPropertyList`

Session Quotas

The following settings appear on the **Session Quotas** tab:

Enable Quota Constraints

If on, then AM allows you to set quota constraints on CTS-based sessions.

The possible values for this property are:

- `ON`

- `OFF`

Default value: `OFF`

amster attribute: `iplanet-am-session-enable-session-constraint`

Read Timeout for Quota Constraint

Maximum wait time after which AM considers a search for live session count as having failed if quota constraints are enabled, in milliseconds.

Default value: `6000`

amster attribute: `quotaConstraintMaxWaitTime`

Resulting behavior if session quota exhausted

Specify the action to take if a session quota is exhausted:

- **Deny Access**. New session creation requests will be denied.
- **Destroy Next Expiring**. The session that would expire next will be destroyed.
- **Destroy Oldest**. The oldest session will be destroyed.
- **Destroy All**. All previous sessions will be destroyed.

The possible values for this property are:

- `org.forgerock.openam.session.service.DenyAccessAction`. Deny Access
- `org.forgerock.openam.session.service.DestroyNextExpiringAction`. Destroy Next Expiring
- `org.forgerock.openam.session.service.DestroyOldestAction`. Destroy Oldest
- `org.forgerock.openam.session.service.DestroyAllAction`. Destroy All

Default value: `org.forgerock.openam.session.service.DestroyNextExpiringAction`

amster attribute: `behaviourWhenQuotaExhausted`

Deny user login when session repository is down

This property only takes effect when the session quota constraint is enabled, and the session data store is unavailable.

The possible values for this property are:

- `YES`
- `NO`

Default value: `NO`

amster attribute: `denyLoginWhenRepoDown`

Client-based Sessions

The following settings appear on the **Client-based Sessions** tab:

Signing Algorithm Type

Specifies the algorithm that AM uses to sign the JSON Web Token (JWT) containing the session content. Signing the JWT enables tampering detection.

AM supports the following signing algorithms:

- **HS256**. HMAC using SHA-256.
- **HS384**. HMAC using SHA-384.
- **HS512**. HMAC using SHA-512.
- **RS256**. RSASSA-PKCS1-v1_5 using SHA-256.
- **ES256**. ECDSA using SHA-256 and NIST standard P-256 elliptic curve.
- **ES384**. ECDSA using SHA-384 and NIST standard P-384 elliptic curve.
- **ES512**. ECDSA using SHA-512 and NIST standard P-521 elliptic curve.

The possible values for this property are:

- `NONE`
- `HS256`
- `HS384`
- `HS512`
- `RS256`
- `ES256`
- `ES384`
- `ES512`

Default value: `HS256`

amster attribute: `statelessSigningType`

Signing HMAC Shared Secret

Specifies the shared secret that AM uses when performing HMAC signing on the session JWT.

Specify a shared secret when using a "Signing Algorithm Type" of `HS256`, `HS384`, or `HS512`.

amster attribute: `statelessSigningHmacSecret`

Encryption Algorithm

Specifies the algorithm that AM uses to encrypt the JSON Web Token (JWT) containing the session content.

AM supports the following encryption algorithms:

- **NONE**. No encryption is selected.
- **RSA**. 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.

  AM supports the following padding modes, which you can set using the `org.forgerock.openam.session.stateless.rsa.padding` advanced property:

  - `RSA1_5`. RSA with PKCS#1 v1.5 padding.
  - `RSA-OAEP`. RSA with optimal asymmetric encryption padding (OAEP) and SHA-1.
  - `RSA-OAEP-256`. RSA with OAEP padding and SHA-256.
- **AES KeyWrapping**. 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 RFC 3394.
- **Direct AES Encryption**. 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.

Important: 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 `org.forgerock.openam.session.stateless.signing.allownone` system property to `true` to turn off signing completely.

The possible values for this property are:

- `NONE`
- `RSA`
- `AES_KEYWRAP`. AES KeyWrapping

- `DIRECT`. Direct AES encryption

Default value: `DIRECT`

amster attribute: `statelessEncryptionType`

Encryption Symmetric AES Key

AES key for use with Direct or AES KeyWrap encryption modes.

The symmetric AES key is a base64-encoded random key.

For direct encryption with `AES-GCM` or for `AES-KeyWrap` with any content encryption method, this should be 128, 192, or 256 bits.

For direct encryption with `AES-CBC-HMAC`, the key should be double those sizes (one half for the AES key, the other have for the HMAC key).

AES key sizes greater than 128 bits require installation of the JCE Unlimited Strength policy files in your JRE.

amster attribute: `statelessEncryptionAesKey`

Compression Algorithm

If enabled the session state is compressed before signing and encryption.

WARNING: Enabling compression may compromise encryption. This may leak information about the content of the session state if encryption is enabled.

The possible values for this property are:

- `NONE`
- `DEF`. Deflate Compression.

Default value: `NONE`

amster attribute: `statelessCompressionType`

Enable Session Blacklisting

Blacklists client-based sessions that log out.

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.

Default value: `false`

amster attribute: `openam-session-stateless-enable-session-blacklisting`

Session Blacklist Cache Size

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.

Default value: `10000`

amster attribute: `openam-session-stateless-blacklist-cache-size`

Blacklist Poll Interval (seconds)

Specifies the interval at which AM polls the Core Token Service to update the list of logged out sessions, in seconds.

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 `0` to disable this feature completely.

Default value: `60`

amster attribute: `openam-session-stateless-blacklist-poll-interval`

Blacklist Purge Delay (minutes)

When added to the maximum session time, specifies the amount of time that AM tracks logged out sessions.

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.

Default value: `1`

amster attribute: `openam-session-stateless-blacklist-purge-delay`

Dynamic Attributes

Note

Configuring any of the following properties at the realm level (Realms > *Realm Name* > Services > Session) causes the values to be stored in the identity store configured in that realm.

If you remove the identity store from the realm, the properties will use the values configured at the global level (Configure > Global Services > Session).

The following settings appear on the **Dynamic Attributes** tab:

Maximum Session Time

Maximum time a session can remain valid before AM requires the user to authenticate again, in minutes.

Default value: `120`

amster attribute: `maxSessionTime`

Maximum Idle Time

Maximum time a CTS-based session can remain idle before AM requires the user to authenticate again, in minutes.

Default value: `30`

amster attribute: `maxIdleTime`

Maximum Caching Time

Maximum time that external clients of AM are recommended to cache the session for, in minutes.

Default value: `3`

amster attribute: `maxCachingTime`

Active User Sessions

Maximum number of concurrent CTS-based sessions AM allows a user to have.

Default value: `5`

amster attribute: `quotaLimit`

Session Property Whitelist Service

amster service name: `SessionPropertyWhiteList`

Realm Defaults

The following settings appear on the **Realm Defaults** tab:

Whitelisted Session Property Names

A list of properties that users may read, edit the value of, or delete from their session.

Adding properties to sessions can impact AM'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 AM deployment in the following areas:

- AM server memory
- OpenDJ storage
- OpenDJ replication

Protected attributes will NOT be allowed to be set, edited or deleted, even if they are included in this whitelist.

Default value: `AMCtxId`

amster attribute: `sessionPropertyWhitelist`

Session Properties to return for session queries

A list of session properties that can be returned to admins in a REST session query response.

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.

Protected attributes will NOT be allowed to be set, edited or deleted, even if they are included in this list.

amster attribute: `whitelistedQueryProperties`

Social Authentication Implementations

amster service name: `SocialAuthentication`

Realm Defaults

The following settings appear on the **Realm Defaults** tab:

Display Names

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.

For example:

Key	Value
google	Google

Default value: `{}`

amster attribute: `displayNames`

Authentication Chains

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.

For example:

Key	Value
google	socialAuthChainGoogle

Default value: `{}`

amster attribute: `authenticationChains`

Icons

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.

For example:

Key	Value
google	/images/google-sign-in.png

Default value: `{}`

amster attribute: `icons`

Enabled Implementations

Provide a key that has been used to define the settings above to enable that set of settings.

For example: google

amster attribute: `enabledKeys`

Social Identity Provider Service

amster service name: `SocialIdentityProviders`

Realm Defaults

The following settings appear on the **Realm Defaults** tab:

Enabled

Default value: `true`

amster attribute: `enabled`

Transaction Authentication Service

amster service name: `TransactionAuthentication`

Realm Defaults

The following settings appear on the **Realm Defaults** tab:

Time to Live

The number of seconds within which the transaction must be completed.

Default value: `180`

amster attribute: `timeToLive`

UMA Provider

amster service name: `UmaProvider`

Realm Defaults

The following settings appear on the **Realm Defaults** tab:

Permission Ticket Lifetime (seconds)

The maximum life of a permission ticket before it expires, in seconds.

Default value: `120`

amster attribute: `permissionTicketLifetime`

Delete user policies when Resource Server is removed

Delete all user policies that relate to a Resource Server when removing the OAuth2 agent entry or removing the `uma_protection` scope from the OAuth2 agent.

Default value: `true`

amster attribute: `deletePoliciesOnDeleteRS`

Delete resources when Resource Server is removed

Delete all resources that relate to a Resource Server when removing the OAuth2 agent entry or removing the `uma_protection` scope from the OAuth2 agent.

Default value: `true`

amster attribute: `deleteResourceSetsOnDeleteRS`

Pending Requests Enabled

Specifies whether to use the Pending Requests subsystem that notifies the resource owner that an attempt to access a resource was made.

Default value: `true`

amster attribute: `pendingRequestsEnabled`

Email Resource Owner on Pending Request creation

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.

Default value: `true`

amster attribute: `emailResourceOwnerOnPendingRequestCreation`

Email Requesting Party on Pending Request approval

Specifies whether to send an email to the Requesting Party when a Pending Request is approved by the Resource Owner.

Default value: `true`

amster attribute: `emailRequestingPartyOnPendingRequestApproval`

User profile preferred Locale attribute

User profile attribute storing the user's preferred locale.

Default value: `inetOrgPerson`

amster attribute: `userProfileLocaleAttribute`

Re-Sharing Mode

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.

The possible values for this property are:

- `OFF`
- `IMPLICIT`

Default value: `IMPLICIT`

amster attribute: `resharingMode`

Grant RPTs...

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.

Default value:

```
REQUEST_PARTIAL
REQUEST_NONE
TICKET_PARTIAL
```

amster attribute: `grantRptConditions`

User

amster service name: `IdRepositoryUser`

Dynamic Attributes

The following settings appear on the **Dynamic Attributes** tab:

User Preferred Timezone

Time zone for accessing AM console.

amster attribute: `preferredTimezone`

Administrator DN Starting View

Specifies the DN for the initial screen when the AM administrator successfully logs in to the AM console.

amster attribute: `adminDNStartingView`

Default User Status

Inactive users cannot authenticate, though AM stores their profiles.

The possible values for this property are:

- `Active`
- `Inactive`

Default value: `Active`

amster attribute: `defaultUserStatus`

User Self-Service

amster service name: `UserSelfService`

General Configuration

The following settings appear on the **General Configuration** tab:

Encryption Key Pair Alias

An encryption key alias in the AM server's JCEKS keystore. Used to encrypt the JWT token that AM uses to track end users during User Self-Service operations.

For example, you might set this property to: *selfserviceenctest*

amster attribute: `encryptionKeyPairAlias`

Signing Secret Key Alias

A signing secret key alias in the AM server's JCEKS keystore. Used to sign the JWT token that AM uses to track end users during User Self-Service operations.

For example, you might set this property to: *selfservicesigntest*

amster attribute: `signingSecretKeyAlias`

Google reCAPTCHA Site Key

Google reCAPTCHA plugin site key.

amster attribute: `captchaSiteKey`

Google reCAPTCHA Secret Key

Google reCAPTCHA plugin secret key.

amster attribute: `captchaSecretKey`

Google Re-captcha Verification URL

Google reCAPTCHA plugin verification URL.

Default value: `https://www.google.com/recaptcha/api/siteverify`

amster attribute: `captchaVerificationUrl`

Security Questions

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.

Format is `unique key|locale|question`.

Default value:

```
4|en|What is your mother's maiden name?
3|en|What was the name of your childhood pet?
2|en|What was the model of your first car?
1|en|What is the name of your favourite restaurant?
```

amster attribute: `kbaQuestions`

Minimum Answers to Define

Specifies the minimum number of KBA answers that users must define.

Default value: `1`

amster attribute: `minimumAnswersToDefine`

Minimum Answers to Verify

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 `0` to `50`.

Default value: `1`

amster attribute: `minimumAnswersToVerify`

Valid Query Attributes

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.

Default value:

```
uid
```

```
mail
givenName
sn
```

amster attribute: `validQueryAttributes`

User Registration

The following settings appear on the **User Registration** tab:

User Registration

If enabled, new users can sign up for an account.

Default value: `false`

amster attribute: `userRegistrationEnabled`

Captcha

If enabled, users must pass a Google reCAPTCHA challenge during user self-registration to mitigate against software bots.

Default value: `false`

amster attribute: `userRegistrationCaptchaEnabled`

Email Verification

If enabled, users who self-register must perform email address verification.

Default value: `true`

amster attribute: `userRegistrationEmailVerificationEnabled`

Verify Email before User Detail

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.

Default value: `false`

amster attribute: `userRegistrationEmailVerificationFirstEnabled`

Security Questions

If enabled, users must set up their security questions during the self-registration process.

Default value: `false`

amster attribute: `userRegistrationKbaEnabled`

Token Lifetime (seconds)

Maximum lifetime of the token allowing User Self-Registration, in seconds.

Default value: `300`

amster attribute: `userRegistrationTokenTTL`

Outgoing Email Subject

Customize the User Self-Registration verification email subject text. Format is `locale|subject text`.

Default value: `en|Registration email`

amster attribute: `userRegistrationEmailSubject`

Outgoing Email Body

Customize the User Self-Registration verification email body text. Format is: `locale|body text`.

Default value: `en|<h2>Click on this <a href="%link%">link</a> to register.</h2>`

amster attribute: `userRegistrationEmailBody`

Valid Creation Attributes

Specifies a whitelist of user attributes that can be set during user creation.

Default value:

```
userPassword
mail
givenName
kbaInfo
inetUserStatus
sn
username
```

amster attribute: `userRegistrationValidUserAttributes`

Destination After Successful Self-Registration

Specifies the action to be taken after a user successfully registers a new account. Choose from:

- `default`. User is sent to a success page without being logged in.
- `login`. User is sent to the login page to authenticate.
- `autologin`. User is automatically logged in and sent to the appropriate page.

The possible values for this property are:

- Label: **User sent to 'successful registration' page** (Value: `default`)
- Label: **User sent to login page** (Value: `login`)
- Label: **User is automatically logged in** (Value: `auto-login`)

Default value: `default`

amster attribute: `userRegisteredDestination`

Forgotten Password

The following settings appear on the **Forgotten Password** tab:

Forgotten Password

If enabled, users can reset their forgotten password.

Default value: `false`

amster attribute: `forgottenPasswordEnabled`

Captcha

If enabled, users must pass a Google reCAPTCHA challenge during password reset to mitigate against software bots.

Default value: `false`

amster attribute: `forgottenPasswordCaptchaEnabled`

Email Verification

If enabled, users who reset passwords must perform email address verification.

Default value: `true`

amster attribute: `forgottenPasswordEmailVerificationEnabled`

Security Questions

If enabled, users must answer their security questions during the forgotten password process.

Default value: `false`

amster attribute: `forgottenPasswordKbaEnabled`

Enforce password reset lockout

If enabled, users will be prevented from resetting their password after the configured number of failed attempts.

Default value: `false`

amster attribute: `numberOfAttemptsEnforced`

Lock Out After number of attempts

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.

Default value: `1`

amster attribute: `numberOfAllowedAttempts`

Token Lifetime (seconds)

Maximum lifetime for the token allowing forgotten password reset, in seconds.

Specify a value from `0` to `2147483647`.

Default value: `300`

amster attribute: `forgottenPasswordTokenTTL`

Outgoing Email Subject

Customize the forgotten password email subject text. Format is `locale|subject text`.

Default value: `en|Forgotten password email`

amster attribute: `forgottenPasswordEmailSubject`

Outgoing Email Body

Customize the forgotten password email body text. Format is `locale|body text`.

Default value: `en|<h2>Click on this <a href="%link%">link</a> to reset your password.</h2>`

amster attribute: `forgottenPasswordEmailBody`

Forgotten Username

The following settings appear on the **Forgotten Username** tab:

Forgotten Username

If enabled, users can retrieve their forgotten username.

Default value: `false`

amster attribute: `forgottenUsernameEnabled`

Captcha

If enabled, users must pass a Google reCAPTCHA challenge during the forgotten username retrieval process to mitigate against software bots.

Default value: `false`

amster attribute: `forgottenUsernameCaptchaEnabled`

Security Questions

If enabled, users must answer their security questions during the forgotten username process.

Default value: `false`

amster attribute: `forgottenUsernameKbaEnabled`

Email Username

If enabled, users receive their forgotten username by email.

Default value: `true`

amster attribute: `forgottenUsernameEmailUsernameEnabled`

Show Username

If enabled, users see their forgotten username on the browser page.

Default value: `false`

amster attribute: `forgottenUsernameShowUsernameEnabled`

Token LifeTime (seconds)

Maximum lifetime for the token allowing forgotten username, in seconds.

Default value: `300`

amster attribute: `forgottenUsernameTokenTTL`

Outgoing Email Subject

Customizes the forgotten username email subject text. Format is `locale|subject text`.

Default value: `en|Forgotten username email`

amster attribute: `forgottenUsernameEmailSubject`

Outgoing Email Body

Customizes the forgotten username email body text. Format is `locale|body text`.

Default value: `en|<h2>Your username is <span style="color:blue">%username%</span>.</h2>`

amster attribute: `forgottenUsernameEmailBody`

Profile Management

The following settings appear on the **Profile Management** tab:

Protected Update Attributes

Specifies a profile's protected user attributes, which causes re-authentication when the user attempts to modify these attributes.

amster attribute: `profileProtectedUserAttributes`

Self readable attributes

Specifies the list of attributes that users can view when accessing their user profile.

Default value:

```
uid
telephoneNumber
mail
kbaInfo
givenName
sn
cn
```

amster attribute: `profileAttributeWhitelist`

Advanced Configuration

The following settings appear on the **Advanced Configuration** tab:

User Registration Confirmation Email URL

Specifies the confirmation URL that the user receives during the self-registration process. The `${realm}` string is replaced with the current realm.

Default value: `http://openam.example.com:8080/openam/XUI/?realm=${realm}#register/`

amster attribute: `userRegistrationConfirmationUrl`

Forgotten Password Confirmation Email URL

Specifies the confirmation URL that the user receives after confirming their identity during the forgotten password process. The `${realm}` string is replaced with the current realm.

Default value: `http://openam.example.com:8080/openam/XUI/?realm=${realm}#passwordReset/`

amster attribute: `forgottenPasswordConfirmationUrl`

User Registration Service Config Provider Class

Specifies the provider class to configure any custom plugins.

Default value: `org.forgerock.openam.selfservice.config.flows.UserRegistrationConfigProvider`

amster attribute: `userRegistrationServiceConfigClass`

Forgotten Password Service Config Provider Class

Specifies the provider class to configure any custom plugins.

Default value: `org.forgerock.openam.selfservice.config.flows.ForgottenPasswordConfigProvider`

amster attribute: `forgottenPasswordServiceConfigClass`

Forgotten Username Service Config Provider Class

Specifies the provider class to configure any custom plugins.

Default value: `org.forgerock.openam.selfservice.config.flows.ForgottenUsernameConfigProvider`

amster attribute: `forgottenUsernameServiceConfigClass`

Self Service Trees

amster service name: `SelfServiceTrees`

Realm Defaults

The following settings appear on the **Realm Defaults** tab:

Enabled

Default value: `true`

amster attribute: `enabled`

Tree Mapping

Maps the self service function name (the key) to an Authentication Tree (the value).

Default value: `{}`

amster attribute: `treeMapping`

Validation Service

amster service name: `ValidationService`

Global Attributes

The following settings appear on the **Global Attributes** tab:

Valid goto URL Resources

List of valid goto URL resources.

Specifies a list of valid URLs for the `goto` and `gotoOnFail` 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, `domain-of-am-instance.com`. Use the `*` wildcard to match all characters except `?`.

Examples:

- `http://app.example.com:80/*`
- `http://app.example.com:80/*?*`

amster attribute: `validGotoDestinations`

Realm Defaults

The following settings appear on the **Realm Defaults** tab:

Valid goto URL Resources

List of valid goto URL resources.

Specifies a list of valid URLs for the `goto` and `gotoOnFail` 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, `domain-of-am-instance.com`. Use the `*` wildcard to match all characters except `?`.

Examples:

- `http://app.example.com:80/*`
- `http://app.example.com:80/*?*`

amster attribute: `validGotoDestinations`

WebAuthn Profile Encryption Service

amster service name: `AuthenticatorWebAuthn`

Realm Defaults

The following settings appear on the **Realm Defaults** tab:

Profile Storage Attribute

The user's attribute in which to store WebAuthn profiles.

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.

Default value: `webauthnDeviceProfiles`

amster attribute: `webauthnAttrName`

Device Profile Encryption Scheme

Encryption scheme to use to secure device profiles stored on the server.

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.

Note: AES-256 may require installation of the JCE Unlimited Strength policy files.

The possible values for this property are:

- Label: **AES-256/HMAC-SHA-512 with RSA Key Wrapping** (Value: `RSAES_AES256CBC_HS512`)
- Label: **AES-128/HMAC-SHA-256 with RSA Key Wrapping** (Value: `RSAES_AES128CBC_HS256`)
- Label: **No encryption of device settings.** (Value: `NONE`)

Default value: `NONE`

amster attribute: `authenticatorWebAuthnDeviceSettingsEncryptionScheme`

Encryption Key Store

Path to the key store from which to load encryption keys.

Default value: `/path/to/openam/security/keystores/keystore.jceks`

amster attribute: `authenticatorWebAuthnDeviceSettingsEncryptionKeystore`

Key Store Type

Type of key store to load.

Note: 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.

See the JDK 8 PKCS#11 Reference Guide for more details.

The possible values for this property are:

- Label: **Java Key Store (JKS).** (Value: `JKS`)
- Label: **Java Cryptography Extension Key Store (JCEKS).** (Value: `JCEKS`)
- Label: **PKCS#11 Hardware Crypto Storage.** (Value: `PKCS11`)
- Label: **PKCS#12 Key Store.** (Value: `PKCS12`)

Default value: `JCEKS`

amster attribute: `authenticatorWebAuthnDeviceSettingsEncryptionKeystoreType`

Key Store Password

Password to unlock the key store. This password is encrypted when it is saved in the AM configuration. You should modify the default value.

amster attribute: `authenticatorWebAuthnDeviceSettingsEncryptionKeystorePassword`

Key-Pair Alias

Alias of the certificate and private key in the key store. The private key is used to encrypt and decrypt device profiles.

amster attribute: `authenticatorWebAuthnDeviceSettingsEncryptionKeystoreKeyPairAlias`

Private Key Password

Password to unlock the private key.

amster attribute: `authenticatorWebAuthnDeviceSettingsEncryptionKeystorePrivateKeyPassword`

Chapter 5
Ports Used

The software uses a number of ports by default.

Default ports are shown in the following table:

Default Ports Used

Port Number	Protocol	Description
1689	TCP/IP	Port for Java Management eXtension traffic, disabled by default
1812	UDP	Port for AM's RADIUS server, disabled by default
4444	TCP/IP	Port for the embedded administration connector, enabled by default.
8080	TCP/IP	Web application container port number
8082	TCP/IP	HTTP port for monitoring AM, disabled by default
8085	TCP/IP	SNMP port for monitoring AM, disabled by default
9999	TCP/IP	RMI port for monitoring AM, disabled by default.
50389, 50899, 58989	TCP/IP	Supports LDAP communication between embedded AM data stores.

Sometimes multiple services are configured on a single system with slightly different port numbers. For example, while the default port number for a servlet container such as Tomcat is 8080, a second instance of Tomcat might be configured with a port number of 18080. In all cases shown, communications proceed using the protocol shown in the table.

When you configure a firewall for AM, make sure to include open ports for any installed and related components, including web services (80, 443), servlet containers (8009, 8080, 8443), and external applications.

Additional ports may be used, depending on other components of your deployment. If you are using external ForgeRock Directory Services servers, see Administrative Access in the DS documentation, for the list of default ports used by DS.

Chapter 6
Supported Standards

AM implements the following RFCs, Internet-Drafts, and standards:

+ *Open Authentication*

  RFC 4226: *HOTP: An HMAC-Based One-Time Password Algorithm*, supported by the OATH authentication module and nodes.

  RFC 6238: *TOTP: Time-Based One-Time Password Algorithm*, supported by the OATH authentication module and nodes.

  See more:

  • Open Authentication

+ *OAuth 2.0*

  RFC 6749: The OAuth 2.0 Authorization Framework

  RFC 6750: The OAuth 2.0 Authorization Framework: Bearer Token Usage

  RFC 7009: OAuth 2.0 Token Revocation

  RFC 7515: JSON Web Signature (JWS)

  RFC 7516: JSON Web Encryption (JWE)

  RFC 7517: JSON Web Key (JWK)

  RFC 7518: JSON Web Algorithms (JWA)

  RFC 7519: JSON Web Token (JWT)

  RFC 7522: Security Assertion Markup Language (SAML) 2.0 Profile for OAuth 2.0 Client Authentication and Authorization Grants

  RFC 7523: JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants

RFC 7591: OAuth 2.0 Dynamic Client Registration Protocol

RFC 7636: Proof Key for Code Exchange by OAuth Public Clients

RFC 7662: OAuth 2.0 Token Introspection

RFC 7800: Proof-of-Possession Key Semantics for JSON Web Tokens (JWTs)

Internet-Draft: OAuth 2.0 Device Flow for Browserless and Input Constrained Devices

Internet-Draft: OAuth 2.0 Mutual TLS Client Authentication and Certificate Bound Access Tokens

RFC 7592: OAuth 2.0 Dynamic Client Registration Management Protocol

Internet Draft: JWT Response for OAuth Token Introspection

RFC 8693: OAuth 2.0 Token Exchange (Access token to access token, access token to ID token, ID token to ID token, and ID token to access token)

See more:

- OAuth 2.0

+ *OpenID Connect 1.0*

OpenID Connect Core 1.0 incorporating errata set 1.

In section 5.6 of this specification, AM supports *Normal Claims*. The optional *Aggregated Claims* and *Distributed Claims* representations are not supported by AM.

OpenID Connect Client Initiated Backchannel Authentication Flow - Core 1.0 draft-02

AM applies the guidelines suggested by the OpenID Financial-grade API (FAPI) Working Group to the implementation of CIBA, which shapes the support of CIBA in AM:

+ *Implementation Decisions Applying to CIBA Support in AM*

- AM only supports the CIBA "poll" mode, not the "push" or "ping" modes.
- AM requires use of confidential clients for CIBA.
- AM requires use of signed JSON-web tokens (JWT) to pass parameters, using one of the following algorithms:
  - `ES256` - ECDSA with SHA-256 and NIST standard P-256 elliptic curve.
  - `PS256` - RSASSA-PSS using SHA-256.

Plain JSON or form parameters for CIBA-related data is not supported.

OpenID Connect Discovery 1.0

OpenID Connect Dynamic Client Registration 1.0

OpenID Connect Session Management 1.0- Draft 05

OpenID Connect Session Management 1.0- Draft 10

OAuth 2.0 Multiple Response Type Encoding Practices

OAuth 2.0 Form Post Response Mode

OpenID Connect Back-Channel Logout 1.0 Draft 06.

AM currently only supports backchannel logout when acting as the provider.

See more:

- OpenID Connect 1.0
- OpenID Connect Basic Client Implementer's Guide 1.0
- OpenID Connect Implicit Client Implementer's Guide 1.0

+ *User-Managed Access (UMA) 2.0*

User-Managed Access (UMA) 2.0 Grant for OAuth 2.0 Authorization

Federated Authorization for User-Managed Access (UMA) 2.0

See more:

- User-Managed Access (UMA) 2.0

+ *Security Assertion Markup Language (SAML) and Federation-Related Standards*

AM supports SAML v2.0; support for SAML v1.1 and v1.0 was removed in AM 7, although WS-Federation functionality still creates assertions in SAML v1.x format.

SAML Specifications are available from the OASIS standards page.

Web Services Federation Language (WS-Federation)

Web Services Description Language (WSDL)

eXtensible Access Control Markup Language (XACML)

See more:

- Security Assertion Markup Language (SAML)

+ *Encryption, Hashing, and Signing*

Assertion encryption:

aes128-cbc
aes192-cbc
aes256-cbc
tripledes-cbc

Assertion signatures:

rsa-sha1
rsa-sha256
rsa-sha384
rsa-sha512

Query string signatures:

rsa-sha1
rsa-sha256
rsa-sha384
rsa-sha512
dsa-sha1
ecdsa-sha1
ecdsa-sha256
ecdsa-sha384
ecdsa-sha512

RFC 2898: *PKCS #5: Password-Based Cryptography Specification Version 2.0*

RFC 3394: *Advanced Encryption Standard (AES) Key Wrap Algorithm*

RFC 7518: *JSON Web Algorithms (JWA)*

Federal Information Processing Standard (FIPS) *Security Requirements for Cryptographic Modules*

+ *Other Standards*

Representational State Transfer (REST)

Simple Object Access Protocol (SOAP)

Recommendation E.146, concerning Mobile Subscriber ISDN Numbers (MSISDN), supported for authentication.

RFC 1271: *Remote Network Monitoring Management Information Base*, supported for monitoring over SNMP.

RFC 2578: *Structure of Management Information Version 2 (SMIv2)*, supported for monitoring over SNMP.

RFC 2616: *Hypertext Transfer Protocol -- HTTP/1.1*.

RFC 2579: *Textual Conventions for SMIv2*, supported for monitoring over SNMP.

RFC 2617: *HTTP Authentication: Basic and Digest Access Authentication*, supported as an authentication module.

RFC 2865: *Remote Authentication Dial In User Service (RADIUS)*, supported as an AM service.

RFC 4510: *Lightweight Directory Access Protocol (LDAP)*, for authentication modules and when accessing data stores.

RFC 5280: *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*, supported for certificate-based authentication.

RFC 5646: *Tags for Identifying Languages*.

RFC 5785: *Defining Well-Known Uniform Resource Identifiers (URIs)*.

RFC 6265: *HTTP State Management Mechanism* regarding HTTP Cookies and `Set-Cookie` header fields.

RFC 7239: *Forwarded HTTP Extension*.

Internet-Draft: *Password Policy for LDAP Directories* (draft 09).

Chapter 7
Service Endpoints

A service endpoint is an entry point to a web service. This chapter lists AM service endpoints that are accessible by default.

If you are certain that a particular AM service endpoint is not used in your deployment, you can block access to the endpoint. For more information, see "*Securing Network Communication*" in the *Security Guide*.

JSP Files

Some AM JSP pages are directly accessible as service endpoints. The following sections describe the files for those JSP pages. Directory paths in this section are relative to AM's deployment path, for example, `/path/to/tomcat/webapps/openam/`.

+ *Top-Level JSP Files*

You will find these files in the top-level directory of AM's deployment path.

`Logback.jsp`

Provides a page to configure debug logging. See "*Debug Logging*" in the *Maintenance Guide* for details.

`encode.jsp`

Provides a page to encode a cleartext password for use in SAML entity configurations.

`getServerInfo.jsp`

Supports requests for server information. This page is used internally by AM.

`isAlive.jsp`

Displays a "Server is ALIVE" message when AM is ready to serve requests.

`proxyidpfinder.jsp`

Supports access to a remote identity provider through the federation broker.

`services.jsp`

Lists service configuration information. Use this page when translating configuration changes made in the console into corresponding **ssoadm** commands.

`showServerConfig.jsp`

Displays system configuration information, including the deployment URL, OS, Java VM, configuration directory, and more.

`validat*.jsp` **pages**

These files serve pages and provide endpoints for the classic, JATO-based UI when testing and verifying SAML v2.0 federation.

+ *User Interface JSP Files*

Some classic, JATO-based UI pages rely on JSP files in the `com_sun_web_ui/jsp/` directory. They are not intended to be used directly as external endpoints.

+ *Authentication JSP Files*

The JSP files in the `config/auth/default*/` directories provide templates and endpoints to serve classic, JATO-based UI pages of the AM console that allow users to authenticate.

To adapt the current UI for your deployment, see the UI Customization Guide instead.

+ *OAuth 2.0 JSP Files*

The JSP file, `oauth2/registerClient.jsp`, provides a template page to register an OAuth 2.0 client application without using the main console.

The JSP files in the `oauth2c/` directory serve the Legacy OAuth 2.0/OpenID Connect authentication module. They are not intended to be used directly as external endpoints.

+ *SAML v2.0 JSP Files*

The JSP files in the `saml2/jsp/` directory provide endpoints used in SAML v2.0 deployments.

See "*Federating Identities*" in the *SAML v2.0 Guide* for descriptions of externally useful endpoints.

+ *WS Federation JSP Files*

The JSP files in the `wsfederation/jsp/` directory provide endpoints used in WS-Federation deployments.

WEB-INF URL Patterns

The AM `.war` file includes a deployment descriptor file, `WEB-INF/web.xml`. The deployment descriptor lists services implemented as servlets, and `<url-pattern>` elements that map services to AM endpoints.

When protecting an AM server, consider blocking external access to unused services based on their URL patterns.

The `WEB-INF/web.xml`file changes from release to release. If you remove endpoints from this file to disable access to parts of the AM configuration, make sure you review `WEB-INF/web.xml` when you upgrade to a new release of AM. Remove the restricted endpoints and decide whether to disable the new endpoints.

For information about securing your deployment by restricting access to endpoints, refer to "How do I remove admin UI access in AM" and "Best practice for blocking the top level realm in a proxy for AM" in the *ForgeRock Knowledge Base*

REST API Endpoints

REST API endpoints are discussed in detail as follows:

Authenticating (REST) in the *Authentication and Single Sign-On Guide*

How to use the AM REST APIs to authenticate to AM.

Policies (REST) in the *Authorization Guide*, Policy Sets (REST) in the *Authorization Guide*, Resource Types (REST) in the *Authorization Guide*, and Policy Set Application Types (REST) in the *Authorization Guide*

How to use the AM REST APIs for policy management.

Requesting Policy Decisions Using REST in the *Authorization Guide*

How to use the AM REST APIs for requesting authorization decisions from AM.

OAuth 2.0 Endpoints in the *OAuth 2.0 Guide*

How to use OAuth 2.0-specific endpoints to request access and refresh tokens, as well as introspecting and revoking them.

OAuth 2.0 Administration and Supporting REST Endpoints in the *OAuth 2.0 Guide*

How to use perform OAuth 2.0 administrative tasks, such as register, read, and delete clients.

OpenID Connect 1.0 Endpoints in the *OpenID Connect 1.0 Guide*

How to use OpenID Connect-specific endpoints to retrieve information about an authenticated user, as well as validate ID tokens and check sessions.

"*Retrieving Forgotten Usernames*" in the *User Self-Service Guide*, "*Resetting Forgotten Passwords*" in the *User Self-Service Guide*, and "*Registering Users*" in the *User Self-Service Guide*

How to use the AM REST APIs for user self-registration and forgotten password reset.

Configuring Realms (REST) in the *Setup Guide*

How to use the AM REST APIs for managing AM identities and realms.

Managing Scripts (REST) in the *Getting Started with Scripting*

How to use the AM REST APIs to manage AM scripts.

Recording Troubleshooting Information in the *Maintenance Guide*

How to use the AM REST APIs to record information that can help you troubleshoot AM.

Consuming REST STS Instances in the *Security Token Service (STS) Guide* and "*Querying, Validating, and Canceling Tokens*" in the *Security Token Service (STS) Guide*

How to use the AM REST APIs to manage AM's Security Token Service, which lets you bridge identities across web and enterprise identity access management (IAM) systems through its token transformation process.

Well-Known Endpoints

The endpoints described in this section are Well-Known URIs supported by AM:

`/.well-known/openid-configuration`

Exposes OpenID Provider configuration by HTTP GET as specified by OpenID Connect Discovery 1.0. No query string parameters are required.

`/uma/.well-known/uma2-configuration`

Exposes User-Managed Access (UMA) configuration by HTTP GET as specified by UMA Profile of OAuth 2.0. No query string parameters are required.

For an example, see "/uma/.well-known/uma2-configuration" in the *User-Managed Access (UMA) 2.0 Guide*.

`/.well-known/webfinger`

Allows a client to retrieve the provider URL for an end user by HTTP GET as specified by OpenID Connect Discovery 1.0.

For an example, see "OpenID Connect Discovery" in the *OpenID Connect 1.0 Guide*.

Chapter 8

Log Files and Messages

This chapter gives information about the different log files and messages for the classic Logging Service, which is based on the Java SDK.

Note

OpenAM 13.0.0 introduced a new REST-based Audit Logging Service, which is an audit logging framework common across all ForgeRock products. The classic Logging Service will be deprecated in a future release.

Log Files

This section describes the different classic Logging Service log files.

Audit Log Files

This chapter describes classic Logging Service audit log files:

Audit logs record information about events. You can adjust the amount of detail in the administrative logs under Configuration > System > Logging.

amAuthentication.access

Contains log data for when users log into and out of an instance, including failed authentications

amAuthentication.error

Contains log data about errors encountered when users login and out of an instance

amConsole.access

Contains data about actions run as the administrator in the console, including changes to realms and policies

amConsole.error

Contains data on errors encountered during administrator sessions

amPolicy.access

Contains data about authorization actions permitted by policies, including policy creation, removal, or modification

amPolicy.error

Contains data on errors encountered during actions related to the policy

amPolicyDelegation.access

Contains data about actions as part of the policy delegation, including any changes to the delegation

amRemotePolicy.access

Contains data about policies accessed remotely

amRest.access

Contains data about access to REST endpoints

amRest.authz

Contains data about authorizations to access REST endpoints

amSSO.access

Contains data about user sessions, including times of access, session time outs, session creation, and session termination for stateful sessions; contains data about session creation and session termination for stateless sessions

CoreToken.access

Contains data about actions run against the core token

CoreToken.error

Contains data on errors encountered regarding the core token

COT.access

Contains data about the circle of trust

COT.error

Contains data on errors encountered for the circle of trust

Entitlement.access

Contains data about entitlement actions or changes

OAuth2Provider.access

Contains data about actions for the OAuth 2.0 provider

OAuth2Provider.error

Contains data about errors encountered by the OAuth 2.0 provider

SAML2.access

Contains data about SAML 2 actions, including changes to assertions, artifacts, response, and requests

SAML2.error

Contains data about errors encountered during SAML 2 actions

SAML.access

Contains data about SAML actions, including changes to assertions, artifacts, response, and requests

SAML.error

Contains data about errors encountered during SAML actions

ssoadm.access

Contains data about actions completed for SSO as admin

WebServicesSecurity.access

Contains data about activity for Web Services Security

WebServicesSecurity.error

Contains data on errors encountered by Web Services Security

WSFederation.access

Contains data about activity for WS Federation, including changes and access information

WSFederation.error

Contains data on errors encountered during WS Federation

Debug Log Files

Debug log files provide information to help troubleshoot problems.

The number of messages logged to the debug log files depends on the debug logging level. The default debug logging level is `Error`. Using other logging levels such as `Warning` or `Message` may increase the number of debug log messages and files.

When configured with the Message logging level, a server instance can produce more than a hundred debug log files. Use the debug log file names to determine the type of troubleshooting information in each file. For example, the command-line interface logs debug messages to the `amCLI` debug file. The OAuth2 provider logs debug messages to the `OAuth2Provider` debug file. The Naming Service logs messages to the `amNaming` debug file.

For information about configuring the location and verbosity of debug log files, see "SNMP Monitoring (Legacy)" in the *Maintenance Guide*.

Log Messages

This section describes log messages.

OpenAM logs the following COT messages.

INVALID_COT_NAME

ID: COT-1

Level: INFO

Description: Invalid circle of trust name.

Data: Realm or organization name, Circle of Trust Name

Triggers: Accessing the circle of trust.

Actions: Check the name and retry accessing the circle of trust.

CONFIG_ERROR_MODIFY_COT_DESCRIPTOR

ID: COT-2

Level: INFO

Description: Configuration error modifying the circle of trust.

Data: Error message, Name of the circle of trust, Realm or organization name

Triggers: Modifying the circle of trust.

Actions: Check COT debug , fmCOT, for more detailed error message.

CONFIG_ERROR_GET_ALL_COT_DESCRIPTOR

ID: COT-3

Level: INFO

Description: Error retreiving all circle of trusts.

Data: Error message, Realm or organization name

Triggers: Getting all circle of trust.

Actions: Check configuration; check debug for more detailed error message.

NO_COT_NAME_CREATE_COT_DESCRIPTOR

ID: COT-4

Level: INFO

Description: Invalid name , error creating the circle of trust.

Data: Realm or organization name

Triggers: Creating the circle of trust.

Actions: Check the name to create circle of trust descriptor.

COT_EXISTS_CREATE_COT_DESCRIPTOR

ID: COT-5

Level: INFO

Description: Circle of Trust exists.

Data: Name of the circle of trust, Realm or organization name

Triggers: Creating the circle of trust.

Actions: Create Circle of Trust with a unique name.

INVALID_COT_TYPE

ID: COT-6

Level: INFO

Description: Circle of Trust Type is invalid

Data: Realm or organization name, Circle of Trust Type

Triggers: Creating the circle of trust.

Actions: The values for Circle of Trust type are IDFF , SAML2. Create Circle of Trust using either of these values.

CONFIG_ERROR_CREATE_COT_DESCRIPTOR

ID: COT-7

Level: INFO

Description: Configuration error while creating circle of trust.

Data: Error message, Entity ID, Realm or organization name

Triggers: Create circle of trust.

Actions: Check the fmCOT debug file for detailed errors.

COT_DESCRIPTOR_CREATED

ID: COT-8

Level: INFO

Description: Circle of trust created.

Data: Name of the circle of trust, Realm or organization name

Triggers: Creating the circle of trust.

NULL_COT_NAME_ADD_COT_DESCRIPTOR

ID: COT-9

Level: INFO

Description: Circle of Trust name is null, error adding to circle of trust.

Data: Realm or organization name

Triggers: Adding to the circle of trust.

Actions: Check the name of the circle of trust.

NULL_ENTITYID_ADD_COT_DESCRIPTOR

ID: COT-10

Level: INFO

Description: Entity Identifier is null , cannot add entity to circle of trust

Data: Realm or organization name

Triggers: Adding to the circle of trust.

Actions: Check the value of entity id.

CONFIG_ERROR_ADD_COT_MEMBER

ID: COT-11

Level: INFO

Description: Error adding entity to the circle of trust.

Data: Error message, Name of the circle of trust, Entity Id, Realm or organization name

Triggers: Adding entity to circle of trust.

Actions: Check COT debug for more detailed error message.

NO_COT_NAME_REMOVE_COT_MEMBER

ID: COT-12

Level: INFO

Description: Null circle of trust name.

Data: Realm or organization name

Triggers: Removing member from the circle of trust.

Actions: Check the name of the circle of trust.

NULL_ENTITYID_REMOVE_COT_MEMBER

ID: COT-13

Level: INFO

Description: Null entity identifier.

Data: Name of the circle of trust, Realm or organization name

Triggers: Removing member from the circle of trust.

Actions: Check the value of the entity identifier.

CONFIG_ERROR_REMOVE_COT_MEMBER

ID: COT-14

Level: INFO

Description: Error while removing entity from the circle of trust.

Data: Error message, Name of the circle of trust, Entity Id, Realm or organization name

Triggers: Removing entity identifier from the circle of trust.

Actions: Check COT debug for more detailed error message.

NULL_COT_NAME_LIST_COT

ID: COT-15

Level: INFO

Description: Null circle of trust name.

Data: Realm or organization name

Triggers: Listing entities in Circle of Trust

Actions: Check the name of the circle of trust.

CONFIG_ERROR_LIST_COT_MEMBER

ID: COT-16

Level: INFO

Description: Error listing providers in the circle of trust.

Data: Error message, Name of the circle of trust, Realm or organization name

Triggers: Listing providers in the circle of trust.

Actions: Check COT debug for more detailed error message.

CONFIG_ERROR_DELETE_COT_DESCRIPTOR

ID: COT-17

Level: INFO

Description: Error while deleting the circle of trust.

Data: Error message, Name of the circle of trust, Realm or organization name

Triggers: Deleting the circle of trust.

Actions: Check COT debug for more detailed error message.

INVALID_NAME_ERROR_DELETE_COT_DESCRIPTOR

ID: COT-18

Level: INFO

Description: Invalid name, cannot delete circle of trust.

Data: Circle of Trust Name, Realm or organization name

Triggers: Deleting the circle of trust.

Actions: Check the circle of trust name and retry deletion.

HAS_ENTITIES_DELETE_COT_DESCRIPTOR

ID: COT-19

Level: INFO

Description: Cannot delete circle of trust which has entities.

Data: Circle of Trust Name, Realm or organization name

Triggers: Deleting the circle of trust.

Actions: Remove all entities from the circle of trust and retry deletion.

INVALID_COT_TYPE_DELETE_COT_DESCRIPTOR

ID: COT-20

Level: INFO

Description: Invalid type cannot delete circle of trust.

Data: Realm or organization name, Circle of Trust Name, Circle of Trust Type

Triggers: Deleting the circle of trust.

Actions: Specify correct Circle of Trust type and retry delete.

COT_DESCRIPTOR_DELETED

ID: COT-21

Level: INFO

Description: Circle of trust deleted.

Data: Name of the circle of trust, Realm or organization name

Triggers: Deleting the circle of trust.

COT_FROM_CACHE

ID: COT-22

Level: FINE

Description: Retrieved the circle of trust from cache.

Data: Name of the circle of trust, Realm or organization name

Triggers: Retreived the circle of trust from cache.

CONFIG_ERROR_GET_COT_DESCRIPTOR

ID: COT-23

Level: INFO

Description: Error while getting the circle of trust from data store.

Data: Error message, Name of the circle of trust, Realm or organization name

Triggers: Retreiving the circle of trust

Actions: Check configuration; check debug for more detailed error message.

CONFIG_ERROR_RETREIVE_COT

ID: COT-24

Level: INFO

Description: Error determining an entity is in a circle of trust.

Data: Error message, Name of the circle of trust, ID of an entity, Realm or organization name

Triggers: Determining an entity is in a circle of trust.

Actions: Check debug for more detailed error message.

COT_DESCRIPTOR_RETRIEVED

ID: COT-25

Level: INFO

Description: Retrieved the circle of trust descriptor.

Data: Name of the circle of trust, Realm or organization name

Triggers: Retrieving the circle of trust under a realm.

OpenAM logs the following SAML2 messages.

INVALID_SP

ID: SAML2-1

Level: INFO

Description: Invalid Service Provider Identifier

Data: Service Provider Entity Identifier

Triggers: Invalid Service Provider,cannot process request

Actions: Check the Service Provider Name.

INVALID_IDP

ID: SAML2-2

Level: INFO

Description: Invalid Identity Provider Identifier

Data: Identity Provider Entity Identifier

Triggers: Invalid Identity Provider,cannot process request

Actions: Check the Identity Provider Name.

SP_METADATA_ERROR

ID: SAML2-3

Level: INFO

Description: Unable to retreive Service Provider Metadata.

Data: Service Provider Entity Identifier

Triggers: Cannot retrieve Service Provider Metadata

Actions: Check the Data Store is accessible .; Check the Realm name.; Check the Service Provider Entity Identifier.

IDP_METADATA_ERROR

ID: SAML2-4

Level: INFO

Description: Unable to retrieve Identity Provider Metadata.

Data: Identity Provider Entity Identifier

Triggers: Cannot retreive Identity Provider Metadata

Actions: Check the Data Store is accessible .; Check the Realm name.; Check the Identity Provider Entity Identifier.

SSO_NOT_FOUND

ID: SAML2-5

Level: INFO

Description: Unable to retrieve SingleSignOnService URL.

Data: Identity Provider Entity Identifier

Triggers: Error retreiving SingleSignOnService URL.

Actions: Check the Data Store is accessible .; Check the Realm name.; Check the Identity Provider Entity Identifier.

REDIRECT_TO_SP

ID: SAML2-6

Level: INFO

Description: Redirecting to SingleSignOnService

Data: SingleSignOnService URL

Triggers: Sending Authentication Request by redirecting to Single SignOn Service URL.

RESPONSE_NOT_FOUND_FROM_CACHE

ID: SAML2-7

Level: INFO

Description: Unable to retrieve Response using Response ID after local login.

Data: Response ID

Triggers: Response doesn't exist in the SP cache.

Actions: Check the SP cache clean up interval configuration.

MISSING_ARTIFACT

ID: SAML2-8

Level: INFO

Description: Unable to retrieve Artifact from HTTP Request.

Triggers: SAMLart is missing from HTTP Request

Actions: Check with sender.; Check web container server log.

RECEIVED_ARTIFACT

ID: SAML2-9

Level: INFO

Description: Received Artifact from HTTP Request.

Data: Artifact value

Triggers: Received Artifact from HTTP Request in the process of Single Sign On using Artifact Profile.

IDP_NOT_FOUND

ID: SAML2-10

Level: INFO

Description: Unable to find Identity Provider Entity ID based on the SourceID in Artifact.

Data: Artifact value, Realm or organization name

Triggers: No matching Identity Provider Entity ID found in meta data configuration.

Actions: Check if Identity Provider's meta data is loaded.

IDP_META_NOT_FOUND

ID: SAML2-11

Level: INFO

Description: Unable to load Identity Provider's meta data.

Data: Realm or organization name, Identity Provider Entity ID

Triggers: Unable to load Identity Provider's meta data.

Actions: Check Identity Provider Entity ID.; Check Realm or organization name.; Check if the identity provider's meta is loaded.

ARTIFACT_RESOLUTION_URL_NOT_FOUND

ID: SAML2-12

Level: INFO

Description: Unable to find Identity Provider's Artifact resolution service URL.

Data: Identity Provider Entity ID

Triggers: Artifact resolution service URL is not defined in Identity Provider's metadata.

Actions: Check Identity Provider's meta data.

CANNOT_CREATE_ARTIFACT_RESOLVE

ID: SAML2-13

Level: INFO

Description: Unable to create ArtifactResolve.

Data: Hosted Service Provider Entity ID, Artifact value

Triggers: Error when creating ArtifactResolve instance.

Actions: Check implementation of ArtifactResolve.

CANNOT_GET_SOAP_RESPONSE

ID: SAML2-14

Level: INFO

Description: Unable to obtain response from SOAP communication with Identity Provider's artifact resolution service.

Data: Hosted Service Provider Entity ID, Identity Provider's Artifact Resolution Service URL

Triggers: Error in SOAP communication.

Actions: Check Identity Provider's Artifact Resolution Service URL.; Check SOAP message authentication requirements for Identity Provider's Artifact Resolution Service.

GOT_RESPONSE_FROM_ARTIFACT

ID: SAML2-15

Level: INFO

Description: Obtained response using artifact profile.

Data: Hosted Service Provider Entity ID, Remote Identity Provider Entity ID, Artifact value, Response xml String if the log level was set to LL_FINE at run time

Triggers: Single Sign On using Artifact Profile.

SOAP_ERROR

ID: SAML2-16

Level: INFO

Description: Unable to obtain Artifact Response due to SOAP error.

Data: Identity Provider Entity ID

Triggers: Error in SOAP communication.

Actions: Check configuration for Identity Provider

SOAP_FAULT

ID: SAML2-17

Level: INFO

Description: Received SOAP Fault instead of Artifact Response.

Data: Identity Provider Entity ID

Triggers: Error in Identity Provider's Artifact Resolution.

Actions: Check Identity Provider; Check debug file for detailed fault info.

TOO_MANY_ARTIFACT_RESPONSE

ID: SAML2-18

Level: INFO

Description: Received too many Artifact Response.

Data: Identity Provider Entity ID

Triggers: Identity Provider sent more than one Artifact Response in SOAPMessage.

Actions: Check Identity Provider

CANNOT_INSTANTIATE_ARTIFACT_RESPONSE

ID: SAML2-19

Level: INFO

Description: Unable to instantiate Artifact Response.

Data: Identity Provider Entity ID

Triggers: Error while instantiating Artifact Response.

Actions: Check Identity Provider; Check debug message for detailed error.

MISSING_ARTIFACT_RESPONSE

ID: SAML2-20

Level: INFO

Description: Unable to obtain Artifact Response from SOAP message.

Data: Identity Provider Entity ID

Triggers: No ArtifactResponse is included in SOAPMessage.

Actions: Check Identity Provider

ARTIFACT_RESPONSE_INVALID_SIGNATURE

ID: SAML2-21

Level: INFO

Description: Unable to verify signature on Artifact Response.

Data: Identity Provider Entity ID

Triggers: Error while trying to verify signature on ArtifactResponse.

Actions: Check configuration for Identity Provider; Check debug file for detailed info

ARTIFACT_RESPONSE_INVALID_INRESPONSETO

ID: SAML2-22

Level: INFO

Description: Invalid InResponseTo attribute in Artifact Response.

Data: Identity Provider Entity ID

Triggers: InResponseTo attribute in Artifact Response is missing or doesn't match with Artifact Resolve ID.

Actions: Check with Identity Provider

ARTIFACT_RESPONSE_INVALID_ISSUER

ID: SAML2-23

Level: INFO

Description: Invalid Issuer in Artifact Response.

Data: Identity Provider Entity ID

Triggers: Issuer in Artifact Response is missing or doesn't match with Identity Provider Entity ID.

Actions: Check with Identity Provider

ARTIFACT_RESPONSE_INVALID_STATUS_CODE

ID: SAML2-24

Level: INFO

Description: Invalid status code in Artifact Response.

Data: Identity Provider Entity ID, Status code if the log level was set to LL_FINE at runtime

Triggers: Status in Artifact Response is missing or status code is not Success.

Actions: Check with Identity Provider

CANNOT_INSTANTIATE_RESPONSE_ARTIFACT

ID: SAML2-25

Level: INFO

Description: Unable to instantiate Respones from Artifact Response.

Data: Identity Provider Entity ID

Triggers: Error occurred while instantiating Response.

Actions: Check debug file for detailed error.

MISSING_SAML_RESPONSE_FROM_POST

ID: SAML2-26

Level: INFO

Description: SAML Response is missing from http post.

Triggers: Parameter SAMLResponse is missing from http POST.

CANNOT_INSTANTIATE_RESPONSE_POST

ID: SAML2-27

Level: INFO

Description: Unable to instantiate Response from POST.

Triggers: Error occurred while instantiating Response.

Actions: Check debug file for more info

CANNOT_DECODE_RESPONSE

ID: SAML2-28

Level: INFO

Description: Unable to decode Response.

Triggers: Error occurred while decoding Response.

Actions: Check debug file for more info

GOT_RESPONSE_FROM_POST

ID: SAML2-29

Level: INFO

Description: Obtained response using POST profile.

Data: Response xml String if the log level was set to LL_FINE at runtime

Triggers: Single Sign On using POST Profile.

FED_INFO_WRITTEN

ID: SAML2-30

Level: INFO

Description: Written federation info.

Data: Username, NameIDInfo value string if the log level was set to LL_FINE at runtime

Triggers: Federation is done.

REDIRECT_TO_IDP

ID: SAML2-31

Level: INFO

Description: Redirect request to IDP.

Data: redirection url

Triggers: Single logout.

NO_ACS_URL

ID: SAML2-32

Level: INFO

Description: Unable to find Assertion Consumer Service URL.

Data: meta alias

Triggers: Single Sign On.

NO_RETURN_BINDING

ID: SAML2-33

Level: INFO

Description: Unable to find return binding.

Data: meta alias

Triggers: Single Sign On.

POST_TO_TARGET_FAILED

ID: SAML2-34

Level: INFO

Description: Unable to post the response to target.

Data: Assertion Consumer Service URL

Triggers: Single Sign On with POST binding.

CANNOT_CREATE_ARTIFACT

ID: SAML2-35

Level: INFO

Description: Unable to create an artifact.

Data: IDP entity ID

Triggers: Single Sign On with Artifact binding.

RECEIVED_AUTHN_REQUEST

ID: SAML2-36

Level: INFO

Description: Received AuthnRequest.

Data: SP entity ID, IDP meta alias, authnRequest xml string

Triggers: Single Sign On.

POST_RESPONSE

ID: SAML2-37

Level: INFO

Description: Post response to SP.

Data: SP entity ID, IDP meta alias, response xml string

Triggers: Single Sign On with POST binding.

SEND_ARTIFACT

ID: SAML2-38

Level: INFO

Description: Send an artifact to SP.

Data: IDP entity ID, IDP realm, redirect URL

Triggers: Single Sign On with Artifact binding.

INVALID_SOAP_MESSAGE

ID: SAML2-39

Level: INFO

Description: Encounter invalid SOAP message in IDP.

Data: IDP entity ID

Triggers: Single Sign On with Artifact binding.

ARTIFACT_RESPONSE

ID: SAML2-40

Level: INFO

Description: The artifact response being sent to SP.

Data: IDP entity ID, artifact string, artifact response

Triggers: Single Sign On with Artifact binding.

GOT_ENTITY_DESCRIPTOR

ID: SAML2-41

Level: FINE

Description: Entity descriptor obtained.

Data: Entity ID, Realm or organization name

Triggers: Obtain entity descriptor.

INVALID_REALM_GET_ENTITY_DESCRIPTOR

ID: SAML2-42

Level: INFO

Description: Invaid realm while getting entity descriptor.

Data: Realm or organization name

Triggers: Obtain entity descriptor.

Actions: Check the Realm name.

GOT_INVALID_ENTITY_DESCRIPTOR

ID: SAML2-43

Level: INFO

Description: Obtained invalid entity descriptor.

Data: Entity ID, Realm or organization name

Triggers: Obtain entity descriptor.

Actions: Delete invalid entity descriptor and import it again.

CONFIG_ERROR_GET_ENTITY_DESCRIPTOR

ID: SAML2-44

Level: INFO

Description: Configuration error while getting entity descriptor.

Data: Error message, Entity ID, Realm or organization name

Triggers: Obtain entity descriptor.

Actions: Check debug message for detailed error.

NO_ENTITY_ID_SET_ENTITY_DESCRIPTOR

ID: SAML2-45

Level: INFO

Description: No entity ID while setting entity descriptor.

Data: Realm or organization name

Triggers: Set entity descriptor.

Actions: Set entity ID in entity descriptor.

INVALID_REALM_SET_ENTITY_DESCRIPTOR

ID: SAML2-46

Level: INFO

Description: Invaid realm while setting entity descriptor.

Data: Realm or organization name

Triggers: Set entity descriptor.

Actions: Check the Realm name.

NO_ENTITY_DESCRIPTOR_SET_ENTITY_DESCRIPTOR

ID: SAML2-47

Level: INFO

Description: Entity descriptor doesn't exist while setting entity descriptor.

Data: Entity ID, Realm or organization name

Triggers: Set entity descriptor.

Actions: Create entity descriptor before set.

SET_ENTITY_DESCRIPTOR

ID: SAML2-48

Level: INFO

Description: Entity descriptor was set.

Data: Entity ID, Realm or organization name

Triggers: Set entity descriptor.

CONFIG_ERROR_SET_ENTITY_DESCRIPTOR

ID: SAML2-49

Level: INFO

Description: Configuration error while setting entity descriptor.

Data: Error message, Entity ID, Realm or organization name

Triggers: Set entity descriptor.

Actions: Check debug message for detailed error.

SET_INVALID_ENTITY_DESCRIPTOR

ID: SAML2-50

Level: INFO

Description: Invalid entity descriptor to set.

Data: Entity ID, Realm or organization name

Triggers: Set entity descriptor.

Actions: Check entity descriptor if it follows the schema.

NO_ENTITY_ID_CREATE_ENTITY_DESCRIPTOR

ID: SAML2-51

Level: INFO

Description: No entity ID while creating entity descriptor.

Data: Realm or organization name

Triggers: Create entity descriptor.

Actions: Set entity ID in entity descriptor.

INVALID_REALM_CREATE_ENTITY_DESCRIPTOR

ID: SAML2-52

Level: INFO

Description: Invaid realm while creating entity descriptor.

Data: Realm or organization name

Triggers: Create entity descriptor.

Actions: Check the Realm name.

ENTITY_DESCRIPTOR_EXISTS

ID: SAML2-53

Level: INFO

Description: Entity descriptor exists while creating entity descriptor.

Data: Entity ID, Realm or organization name

Triggers: Create entity descriptor.

Actions: Delete existing entity descriptor first.

ENTITY_DESCRIPTOR_CREATED

ID: SAML2-54

Level: INFO

Description: Entity descriptor was created.

Data: Entity ID, Realm or organization name

Triggers: Create entity descriptor.

CONFIG_ERROR_CREATE_ENTITY_DESCRIPTOR

ID: SAML2-55

Level: INFO

Description: Configuration error while creating entity descriptor.

Data: Error message, Entity ID, Realm or organization name

Triggers: Create entity descriptor.

Actions: Check debug message for detailed error.

CREATE_INVALID_ENTITY_DESCRIPTOR

ID: SAML2-56

Level: INFO

Description: Invalid entity descriptor to create.

Data: Entity ID, Realm or organization name

Triggers: Create entity descriptor.

Actions: Check entity descriptor if it follows the schema.

INVALID_REALM_DELETE_ENTITY_DESCRIPTOR

ID: SAML2-57

Level: INFO

Description: Invaid realm while deleting entity descriptor.

Data: Realm or organization name

Triggers: Delete entity descriptor.

Actions: Check the Realm name.

NO_ENTITY_DESCRIPTOR_DELETE_ENTITY_DESCRIPTOR

ID: SAML2-58

Level: INFO

Description: Entity descriptor doesn't exist while deleting entity descriptor.

Data: Entity ID, Realm or organization name

Triggers: Delete entity descriptor.

ENTITY_DESCRIPTOR_DELETED

ID: SAML2-59

Level: INFO

Description: Entity descriptor was deleted.

Data: Entity ID, Realm or organization name

Triggers: Delete entity descriptor.

CONFIG_ERROR_DELETE_ENTITY_DESCRIPTOR

ID: SAML2-60

Level: INFO

Description: Configuration error while deleting entity descriptor.

Data: Error message, Entity ID, Realm or organization name

Triggers: Delete entity descriptor.

Actions: Check debug message for detailed error.

GOT_ENTITY_CONFIG

ID: SAML2-61

Level: FINE

Description: Entity config obtained.

Data: Entity ID, Realm or organization name

Triggers: Obtain entity config.

INVALID_REALM_GET_ENTITY_CONFIG

ID: SAML2-62

Level: INFO

Description: Invaid realm while getting entity config.

Data: Realm or organization name

Triggers: Obtain entity config.

Actions: Check the Realm name.

GOT_INVALID_ENTITY_CONFIG

ID: SAML2-63

Level: INFO

Description: Obtained invalid entity config.

Data: Entity ID, Realm or organization name

Triggers: Obtain entity config.

Actions: Delete invalid entity config and import it again.

CONFIG_ERROR_GET_ENTITY_CONFIG

ID: SAML2-64

Level: INFO

Description: Configuration error while getting entity config.

Data: Error message, Entity ID, Realm or organization name

Triggers: Obtain entity config.

Actions: Check debug message for detailed error.

NO_ENTITY_ID_SET_ENTITY_CONFIG

ID: SAML2-65

Level: INFO

Description: No entity ID while setting entity config.

Data: Realm or organization name

Triggers: Set entity config.

Actions: Set entity ID in entity config.

INVALID_REALM_SET_ENTITY_CONFIG

ID: SAML2-66

Level: INFO

Description: Invaid realm while setting entity config.

Data: Realm or organization name

Triggers: Set entity config.

Actions: Check the Realm name.

NO_ENTITY_DESCRIPTOR_SET_ENTITY_CONFIG

ID: SAML2-67

Level: INFO

Description: Entity config doesn't exist while setting entity config.

Data: Entity ID, Realm or organization name

Triggers: Set entity config.

Actions: Create entity descriptor before set entity config.

SET_ENTITY_CONFIG

ID: SAML2-68

Level: INFO

Description: Entity config was set.

Data: Entity ID, Realm or organization name

Triggers: Set entity config.

CONFIG_ERROR_SET_ENTITY_CONFIG

ID: SAML2-69

Level: INFO

Description: Configuration error while setting entity config.

Data: Error message, Entity ID, Realm or organization name

Triggers: Set entity config.

Actions: Check debug message for detailed error.

SET_INVALID_ENTITY_CONFIG

ID: SAML2-70

Level: INFO

Description: Invalid entity config to set.

Data: Entity ID, Realm or organization name

Triggers: Set entity config.

Actions: Check entity config if it follows the schema.

NO_ENTITY_ID_CREATE_ENTITY_CONFIG

ID: SAML2-71

Level: INFO

Description: No entity ID while creating entity config.

Data: Realm or organization name

Triggers: Create entity config.

Actions: Set entity ID in entity config.

INVALID_REALM_CREATE_ENTITY_CONFIG

ID: SAML2-72

Level: INFO

Description: Invaid realm while creating entity config.

Data: Realm or organization name

Triggers: Create entity config.

Actions: Check the Realm name.

NO_ENTITY_DESCRIPTOR_CREATE_ENTITY_CONFIG

ID: SAML2-73

Level: INFO

Description: Entity config doesn't exist while creating entity config.

Data: Entity ID, Realm or organization name

Triggers: Create entity config.

Actions: Create entity descriptor before create entity config.

ENTITY_CONFIG_EXISTS

ID: SAML2-74

Level: INFO

Description: Entity config exists while creating entity config.

Data: Entity ID, Realm or organization name

Triggers: Create entity config.

Actions: Delete existing entity config first.

ENTITY_CONFIG_CREATED

ID: SAML2-75

Level: INFO

Description: Entity config was created.

Data: Entity ID, Realm or organization name

Triggers: Create entity config.

CONFIG_ERROR_CREATE_ENTITY_CONFIG

ID: SAML2-76

Level: INFO

Description: Configuration error while creating entity config.

Data: Error message, Entity ID, Realm or organization name

Triggers: Create entity config.

Actions: Check debug message for detailed error.

CREATE_INVALID_ENTITY_CONFIG

ID: SAML2-77

Level: INFO

Description: Invalid entity config to create.

Data: Entity ID, Realm or organization name

Triggers: Create entity config.

Actions: Check entity config if it follows the schema.

INVALID_REALM_DELETE_ENTITY_CONFIG

ID: SAML2-78

Level: INFO

Description: Invaid realm while deleting entity config.

Data: Realm or organization name

Triggers: Delete entity config.

Actions: Check the Realm name.

NO_ENTITY_CONFIG_DELETE_ENTITY_CONFIG

ID: SAML2-79

Level: INFO

Description: Entity config doesn't exist while deleting entity config.

Data: Entity ID, Realm or organization name

Triggers: Delete entity config.

Actions: Check debug message for detailed error.

ENTITY_CONFIG_DELETED

ID: SAML2-80

Level: INFO

Description: Entity config was deleted.

Data: Entity ID, Realm or organization name

Triggers: Delete entity config.

CONFIG_ERROR_DELETE_ENTITY_CONFIG

ID: SAML2-81

Level: INFO

Description: Configuration error while deleting entity config.

Data: Error message, Entity ID, Realm or organization name

Triggers: Delete entity config.

Actions: Check debug message for detailed error.

INVALID_REALM_GET_ALL_HOSTED_ENTITIES

ID: SAML2-82

Level: INFO

Description: Invaid realm while getting all hosted entities.

Data: Realm or organization name

Triggers: Get all hosted entities.

Actions: Check the Realm name.

CONFIG_ERROR_GET_ALL_HOSTED_ENTITIES

ID: SAML2-83

Level: INFO

Description: Configuration error while getting all hosted entities.

Data: Error message, Realm or organization name

Triggers: Get all hosted entities.

Actions: Check debug message for detailed error.

GOT_ALL_HOSTED_ENTITIES

ID: SAML2-84

Level: FINE

Description: Obtained all hosted entities.

Data: Error message, Realm or organization name

Triggers: Get all hosted entities.

INVALID_REALM_GET_ALL_REMOTE_ENTITIES

ID: SAML2-85

Level: INFO

Description: Invaid realm while getting all remote entities.

Data: Realm or organization name

Triggers: Get all remote entities.

Actions: Check the Realm name.

CONFIG_ERROR_GET_ALL_REMOTE_ENTITIES

ID: SAML2-86

Level: INFO

Description: Configuration error while getting all remote entities.

Data: Error message, Realm or organization name

Triggers: Get all remote entities.

Actions: Check debug message for detailed error.

GOT_ALL_REMOTE_ENTITIES

ID: SAML2-87

Level: FINE

Description: Obtained all remote entities.

Data: Error message, Realm or organization name

Triggers: Get all remote entities.

INVALID_INRESPONSETO_RESPONSE

ID: SAML2-88

Level: INFO

Description: InResponseTo attribute in Response is invalid.

Data: Response ID

Triggers: Service Provider received a Response for Single Sign On.

Actions: Check debug message for detailed error.

INVALID_ISSUER_RESPONSE

ID: SAML2-89

Level: INFO

Description: Issuer in Response is invalid.

Data: Hosted Entity ID, Name of Realm or organization, Response ID

Triggers: Issuer in Response is not configured or not trusted by the hosted provider

Actions: Check configuration.

WRONG_STATUS_CODE

ID: SAML2-90

Level: INFO

Description: Status code in Response was not Success.

Data: Response ID, Status code (if log level is set to LL_FINE)

Triggers: Service provider received a Response with wrong Status code. Most likely an error occurred at Identity Provider.

Actions: Check the status code. Contact Identity Provider if needed.

ASSERTION_NOT_ENCRYPTED

ID: SAML2-91

Level: INFO

Description: Assertion in Response was not encrypted.

Data: Response ID

Triggers: Service provider requested the assertion in Response to be encrypted, but it received a Response with unencrypted assertion(s).

Actions: Check configuration. Notify Identity Provider regarding the requirement.

MISSING_ASSERTION

ID: SAML2-92

Level: INFO

Description: Response had no Assertion.

Data: Response ID

Triggers: Service provider received a Response for Single Sign On, but the response contained no Assertion.

Actions: Check error code of the Response. Notify Identity Provider if needed.

INVALID_ISSUER_ASSERTION

ID: SAML2-93

Level: INFO

Description: Issuer in Assertion is not valid.

Data: Assertion ID

Triggers: Issuer in Assertion for single sign on was not configured at service provider, or not trusted by the service provider.

Actions: Check configuration

MISMATCH_ISSUER_ASSERTION

ID: SAML2-94

Level: INFO

Description: Issuer in Assertion didn't match the Issuer in Response or other Assertions in the Response.

Data: Assertion ID

Triggers: Service provider received Response which had mismatch Issuer inside the Assertion it contained.

Actions: Check debug message

INVALID_SIGNATURE_ASSERTION

ID: SAML2-95

Level: INFO

Description: Assertion is not signed or signature is not valid.

Data: Assertion ID

Triggers: Service provider requested the Assertion to be signed but the assertion received was not; or the signature on the Assertion received was not valid.

Actions: Check configuration; check debug for more detailed error message.

MISSING_SUBJECT_COMFIRMATION_DATA

ID: SAML2-96

Level: INFO

Description: SubjectConfirmationData had no Subject.

Data: Assertion ID

Triggers: Service provider received an Assertion whose SubjectConfirmationData had no Subject.

Actions: Check debug for the Assertion received. Contact Identity Provider if needed.

MISSING_RECIPIENT

ID: SAML2-97

Level: INFO

Description: SubjectConfirmationData had no Recipient.

Data: Assertion ID

Triggers: Service provider received an Assertion whose SubjectConfirmationData had no Recipient.

Actions: Check debug for the Assertion received. Contact Identity Provider if needed.

WRONG_RECIPIENT

ID: SAML2-98

Level: INFO

Description: Service Provider is not the intended recipient.

Data: Assertion ID

Triggers: Service provider received an Assertion. But the provider is not the intended recipient of the Assertion.

Actions: Check debug for the Assertion received. Check meta data. Contact Identity Provider if needed.

INVALID_TIME_SUBJECT_CONFIRMATION_DATA

ID: SAML2-99

Level: INFO

Description: Time in SubjectConfirmationData of the Assertion is invalid.

Data: Assertion ID

Triggers: The assertion service provider received had expired timewise.

Actions: Synchronize the time between service provider and identity provider. Increase the time skew attribute for the service provider in its entity config.

CONTAINED_NOT_BEFORE

ID: SAML2-100

Level: INFO

Description: SubjectConfirmationData of the Assertion had NotBefore.

Data: Assertion ID

Triggers: The assertion service provider received had NotBefore.

Actions: Check debug for the Assertion received. Contact identity provider if needed.

WRONG_INRESPONSETO_ASSERTION

ID: SAML2-101

Level: INFO

Description: Assertion contained wrong InResponseTo attribute.

Data: Assertion ID

Triggers: InResponseTo in Assertion is different from the one in Response. Or Assertion didn't contain InResponseTo, but Response did.

Actions: Check debug for the Assertion received. Contact identity provider if needed.

MISSING_CONDITIONS

ID: SAML2-102

Level: INFO

Description: Assertion contained no Conditions.

Data: Assertion ID

Triggers: Conditions is missing from the Single Sign On Assertion.

Actions: Check debug for the Assertion received. Contact identity provider if needed.

MISSING_AUDIENCE_RESTRICTION

ID: SAML2-103

Level: INFO

Description: Assertion contained no AudienceRestriction.

Data: Assertion ID

Triggers: AudienceRestriction is missing from the Single Sign On Assertion.

Actions: Check debug for the Assertion received. Contact identity provider if needed.

WRONG_AUDIENCE

ID: SAML2-104

Level: INFO

Description: Assertion contained wrong Audience.

Data: Assertion ID

Triggers: This service provider was not the intended audience of the single sign on assertion.

Actions: Check debug for the Assertion received. Check meta data. Contact identity provider if needed.

FOUND_AUTHN_ASSERTION

ID: SAML2-105

Level: INFO

Description: Found authentication assertion in the Response.

Data: Assertion ID, Subject if the log level was set to LL_FINE, SesionIndex if any

Triggers: Both the Response and Assertion(s) inside the Response are valid.

INVALID_SSOTOKEN

ID: SAML2-106

Level: INFO

Description: Invalid SSOToken found in Request.

Data: SSOToken value

Triggers: Initiate Single Logout without SSOToken.

MISSING_ENTITY

ID: SAML2-107

Level: INFO

Description: No entity ID is specified in Request.

Data: EntityID value

Triggers: Initiate Request without EntityID.

Actions: Specify EntityID parameter in request URL.

MISSING_META_ALIAS

ID: SAML2-108

Level: INFO

Description: No metaAlias is specified in Request.

Data: MetaAlias value

Triggers: Initiate Request without metaAlias.

Actions: Specify metaAlias parameter in request URL.

REDIRECT_TO_AUTH

ID: SAML2-109

Level: INFO

Description: Redirect request to authentication page.

Data: URL to Authentication page

Triggers: Initiate Request without SSOToken.

CANNOT_DECODE_REQUEST

ID: SAML2-110

Level: INFO

Description: Can not decode URL encoded Query parameter.

Data: URL encoded Query parameter

Triggers: Initiate to decode incorrectly URL encoded Query parameter.

CANNOT_INSTANTIATE_MNI_RESPONSE

ID: SAML2-111

Level: INFO

Description: Can not instantiate MNI Response with input xml.

Data: Input XML string for MNI Response

Triggers: Initiate parse MNI Response with incorrect XML string.

CANNOT_INSTANTIATE_MNI_REQUEST

ID: SAML2-112

Level: INFO

Description: Can not instantiate MNI Request with input XML.

Data: Input XML string for MNI Request

Triggers: Initiate parse MNI Request with incorrect XML string.

CANNOT_INSTANTIATE_SLO_RESPONSE

ID: SAML2-113

Level: INFO

Description: Can not instantiate SLO Response with input XML.

Data: Input XML string for SLO Response

Triggers: Initiate parse SLO Response with incorrect XML string.

CANNOT_INSTANTIATE_SLO_REQUEST

ID: SAML2-114

Level: INFO

Description: Can not instantiate SLO Request with input XML.

Data: Input XML string for SLO Request

Triggers: Initiate parse SLO Request with incorrect XML string.

MNI_REQUEST_INVALID_SIGNATURE

ID: SAML2-115

Level: INFO

Description: Can not varify signature in MNI Request.

Data: MNI Request with signature

Triggers: Sinature in MNI Request is incorrect.

MNI_RESPONSE_INVALID_SIGNATURE

ID: SAML2-116

Level: INFO

Description: Can not valify signature in MNI Response.

Data: MNI Response with signature

Triggers: Sinature in MNI Response is incorrect.

SLO_REQUEST_INVALID_SIGNATURE

ID: SAML2-117

Level: INFO

Description: Can not valify signature in SLO Request.

Data: SLO Request with signature

Triggers: Sinature in SLO Request is incorrect.

SLO_RESPONSE_INVALID_SIGNATURE

ID: SAML2-118

Level: INFO

Description: Can not valify signature in SLO Response.

Data: SLO Response with signature

Triggers: Sinature in SLO Response is incorrect.

NAMEID_INVALID_ENCRYPTION

ID: SAML2-119

Level: INFO

Description: Can not decrypt EncryptedID.

Data: Exception message

Triggers: Decrypt the incorrectly encrypted EncryptedID.

INVALID_MNI_RESPONSE

ID: SAML2-120

Level: INFO

Description: MNI Response has error status.

Data: Status message

Triggers: Requested MNI Request caused problem.

INVALID_SLO_RESPONSE

ID: SAML2-121

Level: INFO

Description: SLO Response has error status.

Data: Status message

Triggers: Requested SLO Request caused problem.

MISSING_ENTITY_ROLE

ID: SAML2-122

Level: INFO

Description: Entity Role is not specified in the request.

Data: Entity Role value

Triggers: Initiate request without Role value.

Actions: Specify Entity Role parameter in the request.

INVALID_ISSUER_REQUEST

ID: SAML2-123

Level: INFO

Description: Issuer in Request is invalid.

Data: Hosted Entity ID, Name of Realm or organization, Request ID

Triggers: Issuer in Request is not configured or not trusted by the hosted provider

Actions: Check configuration.

INVALID_REALM_GET_ALL_ENTITIES

ID: SAML2-124

Level: INFO

Description: Invaid realm while getting all entities.

Data: Realm or organization name

Triggers: Get all entities.

Actions: Check the Realm name.

CONFIG_ERROR_GET_ALL_ENTITIES

ID: SAML2-125

Level: INFO

Description: Configuration error while getting all entities.

Data: Error message, Realm or organization name

Triggers: Get all entities.

Actions: Check debug message for detailed error.

GOT_ALL_ENTITIES

ID: SAML2-126

Level: FINE

Description: Obtained all entities.

Data: Realm or organization name

Triggers: Get all entities.

INVALID_PEP_ID

ID: SAML2-127

Level: INFO

Description: Invalid Policy Enforcement Point (PEP) Identifier.

Data: PEP Identifier

Triggers: Cannot retrieve PEP Metadata

Actions: Provide valid PEP Identifier and retry.

INVALID_PDP_ID

ID: SAML2-128

Level: INFO

Description: Invalid Policy Decision Point (PDP) Identifier.

Data: PDP Identifier

Triggers: Cannot retrieve PDP Metadata

Actions: Provide valid PDP Identifier and retry.

NULL_PDP_SIGN_CERT_ALIAS

ID: SAML2-129

Level: INFO

Description: Certificate Alias is null, cannot sign the message.

Data: The realm from which the metadata was retreived., Entity Identifier for the Policy Decision Point.

Triggers: Cannot sign the message.

Actions: Check the entity's metadata to verify the certificate alias is correct.

NULL_PEP_SIGN_CERT_ALIAS

ID: SAML2-130

Level: INFO

Description: Certificate Alias is null,cannot retreive the certificate.

Data: The realm from which the metadata was retreived., Entity Identifier for the Policy Enforcement Point.

Triggers: Cannot validate the signature in the request message.

Actions: Check the entity's metadata to verify the certificate alias is correct.

INVALID_SIGNATURE_QUERY

ID: SAML2-131

Level: INFO

Description: Invalid Signature in Query Request.

Data: The realm from which the metadata was retreived., Entity Identifier for the Policy Decision Point., Cert Alias used to retrieve certificate from keystore.

Triggers: Cannot process the request, server will send back error to the Requester.

Actions: Check the entity's metadata to verify the certificate alias is correct.; Check the certificate in the keystore for its existance and validity.

INVALID_ISSUER_IN_PEP_REQUEST

ID: SAML2-132

Level: INFO

Description: Issuer in Request is invalid.

Data: Name of Realm or organization, Identity of the Issuer, Hosted Entity Identifier

Triggers: Issuer in Request is not configured or not trusted by the hosted provider therefore Query will fail.

Actions: Check the hosted entity configuration attribute cotlist to make sure the issuer identifier is in the list.

PEP_METADATA_ERROR

ID: SAML2-133

Level: INFO

Description: Unable to retreive Policy Enforcement Point (PEP) Metadata.

Data: PEP Provider Entity Identifier

Triggers: Cannot retrieve PEP Provider Metadata

Actions: Check the Data Store is accessible .; Check the PEP Provider Entity Identifier.

PDP_METADATA_ERROR

ID: SAML2-134

Level: INFO

Description: Unable to retrieve Policy Decision Point (PDP) Metadata.

Data: PDP Provider Entity Identifier

Triggers: Cannot retreive PDP Provider Metadata

Actions: Check the Data Store is accessible .; Check the PDP Provider Entity Identifier.

ASSERTION_FROM_PDP_NOT_ENCRYPTED

ID: SAML2-135

Level: INFO

Description: Assertion in Response not encrypted.

Data: Identity of the Issuer, Response ID

Triggers: Policy Enforcement Point (PEP) Provider requested the assertion in Response to be encrypted, but it received a Response with unencrypted assertion(s).

Actions: Check PEP metadata published to the PDP. Notify Policy Decision Point (PDP) Provider regarding the requirement.

MISSING_ASSERTION_IN_PDP_RESPONSE

ID: SAML2-136

Level: INFO

Description: Response has no Assertion.

Data: Identity of Issuer, Response ID

Triggers: Policy Enforcement Point (PEP) Provider received a Response with no Assertion.

Actions: Check error code of the Response. Notify Policy Decision Point (PDP) Provider to check for errors or possible misconfiguration.

INVALID_ISSUER_IN_ASSERTION_FROM_PDP

ID: SAML2-137

Level: INFO

Description: Issuer in Assertion is not valid.

Data: Assertion Issuer, Assertion ID

Triggers: Issuer in Assertion was not configured at Policy Enforcement Point (PEP) provider, or not trusted by the PEP provider.

Actions: Check the configuration.

MISMATCH_ISSUER_IN_ASSERTION_FROM_PDP

ID: SAML2-138

Level: INFO

Description: Issuer in Assertion doesn't match the Issuer in Response.

Data: Issuer Identifier in the Resposnse, Issuer Identity in the Assertion

Triggers: Error condition, Response will not be accepted.

Actions: Check the Policy Decision Point instance to debug the cause of the problem.

INVALID_SIGNATURE_ASSERTION_FROM_PDP

ID: SAML2-139

Level: INFO

Description: Assertion is not signed or signature is not valid.

Data: Issuer Identity in the Assertion, Assertion ID

Triggers: Policy Enforcement Point (PEP) provider requested the Assertion to be signed but the assertion received was not; or the signature on the Assertion received was not valid.

Actions: Check PEP metadata configuration.; Check debug for more detailed error message.

REQUEST_MESSAGE

ID: SAML2-140

Level: FINE

Description: Request message from Query Requester

Data: policy decision point entity descriptor, SAMLv2 Query Request Message

Triggers: SAMLv2 SOAP Query

VALID_SIGNATURE_QUERY

ID: SAML2-141

Level: INFO

Description: Valid Signature in Query Request.

Data: The realm from which the metadata was retreived., Entity Identifier for the Policy Decision Point., Cert Alias used to retrieve certificate from keystore.

Triggers: The Request will be processed.

SUCCESS_FED_SSO

ID: SAML2-142

Level: INFO

Description: Successful federation/Single Sign On.

Data: user id, NameID value

Triggers: Successful federation/Single Sign On.

SAE_IDP_SUCCESS

ID: SAML2-143

Level: INFO

Description: SAE_IDP succeeded.

Data: SAE attributes

Triggers: SAE_IDP succeeded.

SAE_IDP_ERROR

ID: SAML2-144

Level: INFO

Description: SAE_IDP failed.

Data: Error message, SAE attributes

Triggers: SAE_IDP failed.

SAE_IDP_ERROR_NODATA

ID: SAML2-145

Level: INFO

Description: SAE_IDP invoked without attributes.

Data: Error message

Triggers: SAE_IDP invoked without attributes.

Actions: Add SAE attributes to request.

SAE_IDP_AUTH

ID: SAML2-146

Level: INFO

Description: SAE_IDP delegated to Auth.

Data: SAE attributes

Triggers: SAE_IDP invoked but no user session.

SAE_SP_SUCCESS

ID: SAML2-147

Level: INFO

Description: SAE_SP succeeded.

Data: SAE attributes

Triggers: SAE_SP succeeded.

SAE_SP_ERROR

ID: SAML2-148

Level: INFO

Description: SAE_SP failed.

Data: Error message

Triggers: SAE_SP failed.

SEND_ECP_RESPONSE

ID: SAML2-149

Level: INFO

Description: Send a response to ECP.

Data: Identity Provider Entity Identifier, Realm or organization name, Assertion Consumer Service URL, SOAP message string if the log level was set to LL_FINE at run time

Triggers: Received AuthnRequest.

SEND_ECP_RESPONSE_FAILED

ID: SAML2-150

Level: INFO

Description: Unable to send a response to ECP.

Data: Identity Provider Entity Identifier, Realm or organization name, Assertion Consumer Service URL

Triggers: Send a response to ECP.

CANNOT_INSTANTIATE_SOAP_MESSAGE_ECP

ID: SAML2-151

Level: INFO

Description: Unable to instantiate a SOAP message sent from ECP.

Data: Service Provider Entity Identifier

Triggers: Received a response from ECP.

RECEIVE_SOAP_FAULT_ECP

ID: SAML2-152

Level: INFO

Description: Received a SOAP fault from ECP.

Data: Service Provider Entity Identifier

Triggers: Received a response from ECP.

CANNOT_INSTANTIATE_SOAP_MESSAGE_ECP

ID: SAML2-153

Level: INFO

Description: Unable to instantiate a SAML Response sent from ECP.

Data: Service Provider Entity Identifier

Triggers: Received a response from ECP.

ECP_ASSERTION_NOT_SIGNED

ID: SAML2-154

Level: INFO

Description: Assertion received from ECP is not signed.

Data: Identity Provider Entity Identifier

Triggers: Received a response from ECP.

ECP_ASSERTION_INVALID_SIGNATURE

ID: SAML2-155

Level: INFO

Description: Assertion received from ECP has invalid signature.

Data: Identity Provider Entity Identifier

Triggers: Assertion signature verification.

RECEIVED_AUTHN_REQUEST_ECP

ID: SAML2-156

Level: INFO

Description: Received AuthnRequest from ECP.

Data: Service Provider Entity Identifier, IDP meta alias, authnRequest xml string

Triggers: Single Sign On.

RECEIVED_HTTP_REQUEST_ECP

ID: SAML2-157

Level: INFO

Description: Received HTTP request from ECP.

Data: Service Provider Entity Identifier, Realm or organization name

Triggers: ECP accessed SP Resource.

SEND_ECP_PAOS_REQUEST

ID: SAML2-158

Level: INFO

Description: Send a PAOS request to ECP.

Data: Service Provider Entity Identifier, Realm or organization name, SOAP message string if the log level was set to LL_FINE at run time

Triggers: Received HTTP request from ECP.

SEND_ECP_PAOS_REQUEST_FAILED

ID: SAML2-159

Level: INFO

Description: Unable to send a PAOS request to ECP.

Data: Service Provider Entity Identifier, Realm or organization name

Triggers: Send a PAOS request to ECP.

SUCCESS_FED_TERMINATION

ID: SAML2-160

Level: INFO

Description: Federation termination succeeded.

Data: user id

Triggers: Federation termination succeeded.

SUCCESS_NEW_NAMEID

ID: SAML2-161

Level: INFO

Description: New name identifier succeeded.

Data: user id

Triggers: New name identifier succeeded.

UNKNOWN_PRINCIPAL

ID: SAML2-162

Level: INFO

Description: Unknown princial in manage name ID request.

Data: Manage Name ID request XML

Triggers: Unable to find old name id in the management name id request.

UNABLE_TO_TERMINATE

ID: SAML2-163

Level: INFO

Description: Unable to terminate federation.

Data: user id

Triggers: Unable to terminate federation.

POST_RESPONSE_INVALID_SIGNATURE

ID: SAML2-164

Level: INFO

Description: Unable to verify signature in Single Sign-On Response using POST binding.

Data: Identity Provider Entity ID

Triggers: Error while trying to verify signature in Response.

Actions: Check Identity Provider metadata; Check debug file for detailed info

BINDING_NOT_SUPPORTED

ID: SAML2-165

Level: INFO

Description: Binding is not supported.

Data: Provider Entity ID, Name of binding that is not supported

Triggers: Hosted provider received data from unsupported binding endpoint.

Actions: Check Provider metadata; Check debug file for detailed info

SP_SSO_FAILED

ID: SAML2-166

Level: INFO

Description: Single Sign-On Failed at Service Provider.

Data: Hosted Service Provider Entity ID, Error message, Response received from IDP if the log level was set to LL_FINE at run time

Triggers: Single Sign On failed

Actions: Check debug file for detailed info

INVALID_REALM_FOR_SESSION

ID: SAML2-167

Level: INFO

Description: Invalid realm for the user trying to get an assertion from the IdP.

Data: Realm of the authenticated user, Realm where the IdP is defined, Entity Id of the SP, IP Address of the requester, SAML2 Authentication Request

Triggers: Single Sign On failed

Actions: Check debug file for detailed info

DATE_CONDITION_NOT_MET

ID: SAML2-168

Level: INFO

Description: Assertion NotBefore or NotOnOrAfter condition not met.

Data: Assertion ID

Triggers: The NotBefore or NotOnOrAfter condition of the single sign on assertion was not met.

Actions: Check debug for the Assertion received. Check assertion clock skew. Contact identity provider if needed.

OpenAM logs the following WSFederation messages.

INVALID_SIGNATURE_ASSERTION

ID: WSFederation-1

Level: INFO

Description: Assertion is not signed or signature is not valid.

Data: Assertion or assertion ID, Realm or organization name, Assertion issuer

Triggers: Service provider requested the Assertion to be signed but the assertion received was not; or the signature on the Assertion received was not valid.

Actions: Check configuration; check debug for more detailed error message.

MISSING_CONDITIONS_NOT_ON_OR_AFTER

ID: WSFederation-2

Level: INFO

Description: Assertion conditions are missing notOnOrAfter attribute.

Data: Assertion or assertion ID

Triggers: The Conditions element of the assertion is missing its notOnOrAfter attribute.

Actions: Check the assertion. Contact Identity Provider if needed.

ASSERTION_EXPIRED

ID: WSFederation-3

Level: INFO

Description: Assertion has expired.

Data: Assertion or assertion ID, Assertion notOnOrAfter time, Time skew in seconds, Current time

Triggers: The current time is after the assertion's notOnOrAfter time plus the time skew.

Actions: Synchronize server clocks. Contact Identity Provider if needed.

MISSING_CONDITIONS_NOT_BEFORE

ID: WSFederation-4

Level: INFO

Description: Assertion conditions are missing notBefore attribute.

Data: Assertion or assertion ID

Triggers: The Conditions element of the assertion is missing its notBefore attribute.

Actions: Check the assertion. Contact Identity Provider if needed.

ASSERTION_NOT_YET_VALID

ID: WSFederation-5

Level: INFO

Description: Assertion not yet valid.

Data: Assertion or assertion ID, Assertion notBefore time, Time skew in seconds, Current time

Triggers: The current time is before the assertion's notBefore time minus the time skew.

Actions: Synchronize server clocks. Contact Identity Provider if needed.

MISSING_WRESULT

ID: WSFederation-6

Level: INFO

Description: WS-Federation response is missing wresult.

Data: WS-Federation response

Triggers: The WS-Federation response is missing its wresult parameter.

Actions: Check the response. Contact Identity Provider if needed.

MISSING_WCTX

ID: WSFederation-7

Level: INFO

Description: WS-Federation response is missing wctx.

Data: WS-Federation response

Triggers: The WS-Federation response is missing its wctx parameter.

Actions: Check the response. Contact Identity Provider if needed.

INVALID_WRESULT

ID: WSFederation-8

Level: INFO

Description: WS-Federation response is invalid.

Data: WS-Federation response

Triggers: The WS-Federation response is not a valid RequestSecurityTokenResponse element.

Actions: Check the response. Contact Identity Provider if needed.

CONFIG_ERROR_GET_ENTITY_CONFIG

ID: WSFederation-9

Level: INFO

Description: Configuration error while getting entity config.

Data: Error message, MetaAlias, Realm or organization name

Triggers: Obtain entity config.

Actions: Check debug message for detailed error.

CANT_FIND_SP_ACCOUNT_MAPPER

ID: WSFederation-10

Level: INFO

Description: Can't find SP Account Mapper.

Data: Error message, Account mapper class name

Triggers: Cannot get class object for SP account mapper class.

Actions: Check the configuration. Ensure that SP account mapper class name is correct and that the account mapper class is on the classpath.

CANT_CREATE_SP_ACCOUNT_MAPPER

ID: WSFederation-11

Level: INFO

Description: Can't create SP Account Mapper.

Data: Error message, Account mapper class name

Triggers: Cannot create SP account mapper object.

Actions: Check the configuration. Ensure that SP account mapper class name is correct and that the account mapper class is on the classpath.

CANT_CREATE_SESSION

ID: WSFederation-12

Level: INFO

Description: Can't create session for user.

Data: Error message, Realm or organization name, User name, Auth level

Triggers: Cannot create session for user.

Actions: Check the configuration. Ensure that SP account mapper is finding a user in the local store.

SSO_SUCCESSFUL

ID: WSFederation-13

Level: INFO

Description: Single sign-on completed successfully.

Data: wctx, Assertion or assertion ID, Realm or organization name, User ID, Authentication Level, Target URL

Triggers: Successful WS-Federation RP Signin Response.

UNTRUSTED_ISSUER

ID: WSFederation-14

Level: INFO

Description: Assertion issuer is not trusted by this service provider.

Data: Assertion or assertion ID, Realm or organization name, Service provider ID, Target URL

Triggers: Cannot create session for user.

Actions: Check the configuration. Ensure that SP account mapper is finding a user in the local store.

MISSING_SUBJECT

ID: WSFederation-15

Level: INFO

Description: Assertion does not contain a subject element.

Data: Assertion or assertion ID

Triggers: Assertion does not contain a subject element.

Actions: Check the assertion. Contact Identity Provider if needed.

GOT_FEDERATION

ID: WSFederation-16

Level: FINE

Description: Federation obtained.

Data: Federation ID, Realm or organization name

Triggers: Obtain federation.

GOT_INVALID_ENTITY_DESCRIPTOR

ID: WSFederation-17

Level: INFO

Description: Obtained invalid entity descriptor.

Data: Entity ID, Realm or organization name

Triggers: Obtain entity descriptor.

Actions: Delete invalid entity descriptor and import it again.

CONFIG_ERROR_GET_ENTITY_DESCRIPTOR

ID: WSFederation-18

Level: INFO

Description: Configuration error while getting entity descriptor.

Data: Error message, Entity ID, Realm or organization name

Triggers: Obtain entity descriptor.

Actions: Check debug message for detailed error.

SET_ENTITY_DESCRIPTOR

ID: WSFederation-19

Level: INFO

Description: Entity descriptor was set.

Data: Entity ID, Realm or organization name

Triggers: Set entity descriptor.

CONFIG_ERROR_SET_ENTITY_DESCRIPTOR

ID: WSFederation-20

Level: INFO

Description: Configuration error while setting entity descriptor.

Data: Error message, Entity ID, Realm or organization name

Triggers: Set entity descriptor.

Actions: Check debug message for detailed error.

SET_INVALID_ENTITY_DESCRIPTOR

ID: WSFederation-21

Level: INFO

Description: Invalid entity descriptor to set.

Data: Entity ID, Realm or organization name

Triggers: Set entity descriptor.

Actions: Check entity descriptor if it follows the schema.

ENTITY_DESCRIPTOR_CREATED

ID: WSFederation-22

Level: INFO

Description: Entity descriptor was created.

Data: Entity ID, Realm or organization name

Triggers: Create entity descriptor.

CONFIG_ERROR_CREATE_ENTITY_DESCRIPTOR

ID: WSFederation-23

Level: INFO

Description: Configuration error while creating entity descriptor.

Data: Error message, Entity ID, Realm or organization name

Triggers: Create entity descriptor.

Actions: Check debug message for detailed error.

CREATE_INVALID_ENTITY_DESCRIPTOR

ID: WSFederation-24

Level: INFO

Description: Invalid entity descriptor to create.

Data: Entity ID, Realm or organization name

Triggers: Create entity descriptor.

Actions: Check entity descriptor if it follows the schema.

ENTITY_DESCRIPTOR_DELETED

ID: WSFederation-25

Level: INFO

Description: Entity descriptor was deleted.

Data: Entity ID, Realm or organization name

Triggers: Delete entity descriptor.

CONFIG_ERROR_DELETE_ENTITY_DESCRIPTOR

ID: WSFederation-26

Level: INFO

Description: Configuration error while deleting entity descriptor.

Data: Error message, Entity ID, Realm or organization name

Triggers: Delete entity descriptor.

Actions: Check debug message for detailed error.

GOT_ENTITY_CONFIG

ID: WSFederation-27

Level: FINE

Description: Entity config obtained.

Data: Entity ID, Realm or organization name

Triggers: Obtain entity config.

GOT_INVALID_ENTITY_CONFIG

ID: WSFederation-28

Level: INFO

Description: Obtained invalid entity config.

Data: Entity ID, Realm or organization name

Triggers: Obtain entity config.

Actions: Delete invalid entity config and import it again.

CONFIG_ERROR_GET_ENTITY_CONFIG

ID: WSFederation-29

Level: INFO

Description: Configuration error while getting entity config.

Data: Error message, Entity ID, Realm or organization name

Triggers: Obtain entity config.

Actions: Check debug message for detailed error.

NO_ENTITY_ID_SET_ENTITY_CONFIG

ID: WSFederation-30

Level: INFO

Description: No entity ID while setting entity config.

Data: Realm or organization name

Triggers: Set entity config.

Actions: Set entity ID in entity config.

SET_ENTITY_CONFIG

ID: WSFederation-31

Level: INFO

Description: Entity config was set.

Data: Entity ID, Realm or organization name

Triggers: Set entity config.

CONFIG_ERROR_SET_ENTITY_CONFIG

ID: WSFederation-32

Level: INFO

Description: Configuration error while setting entity config.

Data: Error message, Entity ID, Realm or organization name

Triggers: Set entity config.

Actions: Check debug message for detailed error.

SET_INVALID_ENTITY_CONFIG

ID: WSFederation-33

Level: INFO

Description: Invalid entity config to set.

Data: Entity ID, Realm or organization name

Triggers: Set entity config.

Actions: Check entity config if it follows the schema.

NO_ENTITY_ID_CREATE_ENTITY_CONFIG

ID: WSFederation-34

Level: INFO

Description: No entity ID while creating entity config.

Data: Realm or organization name

Triggers: Create entity config.

Actions: Set entity ID in entity config.

NO_ENTITY_DESCRIPTOR_CREATE_ENTITY_CONFIG

ID: WSFederation-35

Level: INFO

Description: Entity config doesn't exist while creating entity config.

Data: Entity ID, Realm or organization name

Triggers: Create entity config.

Actions: Create entity descriptor before create entity config.

ENTITY_CONFIG_EXISTS

ID: WSFederation-36

Level: INFO

Description: Entity config exists while creating entity config.

Data: Entity ID, Realm or organization name

Triggers: Create entity config.

Actions: Delete existing entity config first.

ENTITY_CONFIG_CREATED

ID: WSFederation-37

Level: INFO

Description: Entity config was created.

Data: Entity ID, Realm or organization name

Triggers: Create entity config.

CONFIG_ERROR_CREATE_ENTITY_CONFIG

ID: WSFederation-38

Level: INFO

Description: Configuration error while creating entity config.

Data: Error message, Entity ID, Realm or organization name

Triggers: Create entity config.

Actions: Check debug message for detailed error.

CREATE_INVALID_ENTITY_CONFIG

ID: WSFederation-39

Level: INFO

Description: Invalid entity config to create.

Data: Entity ID, Realm or organization name

Triggers: Create entity config.

Actions: Check entity config if it follows the schema.

NO_ENTITY_CONFIG_DELETE_ENTITY_CONFIG

ID: WSFederation-40

Level: INFO

Description: Entity config doesn't exist while deleting entity config.

Data: Entity ID, Realm or organization name

Triggers: Delete entity config.

Actions: Check debug message for detailed error.

ENTITY_CONFIG_DELETED

ID: WSFederation-41

Level: INFO

Description: Entity config was deleted.

Data: Entity ID, Realm or organization name

Triggers: Delete entity config.

CONFIG_ERROR_DELETE_ENTITY_CONFIG

ID: WSFederation-42

Level: INFO

Description: Configuration error while deleting entity config.

Data: Error message, Entity ID, Realm or organization name

Triggers: Delete entity config.

Actions: Check debug message for detailed error.

CONFIG_ERROR_GET_ALL_HOSTED_ENTITIES

ID: WSFederation-43

Level: INFO

Description: Configuration error while getting all hosted entities.

Data: Error message, Realm or organization name

Triggers: Get all hosted entities.

Actions: Check debug message for detailed error.

GOT_ALL_HOSTED_ENTITIES

ID: WSFederation-44

Level: FINE

Description: Obtained all hosted entities.

Data: Realm or organization name

Triggers: Get all hosted entities.

CONFIG_ERROR_GET_ALL_REMOTE_ENTITIES

ID: WSFederation-45

Level: INFO

Description: Configuration error while getting all remote entities.

Data: Error message, Realm or organization name

Triggers: Get all remote entities.

Actions: Check debug message for detailed error.

GOT_ALL_REMOTE_ENTITIES

ID: WSFederation-46

Level: FINE

Description: Obtained all remote entities.

Data: Error message, Realm or organization name

Triggers: Get all remote entities.

CONFIG_ERROR_GET_ALL_ENTITIES

ID: WSFederation-47

Level: INFO

Description: Configuration error while getting all entities.

Data: Error message, Realm or organization name

Triggers: Get all entities.

Actions: Check debug message for detailed error.

GOT_ALL_ENTITIES

ID: WSFederation-48

Level: FINE

Description: Obtained all entities.

Data: Realm or organization name

Triggers: Get all entities.

ASSERTION_CREATED

ID: WSFederation-49

Level: INFO

Description: Assertion created successfully.

Data: Assertion or assertion ID

Triggers: Creation of WS-Federation IdP Signin Response.

NO_ACS_URL

ID: WSFederation-50

Level: INFO

Description: Could not find an Assertion Consumer Service URL.

Data: Realm or organization name, Service provider ID, Reply URL

Triggers: No ACS URL in configuration.; ACS URL provided in request not found in configuration.

Actions: Check configuration for service provider.

SLO_SUCCESSFUL

ID: WSFederation-51

Level: INFO

Description: Single logout completed successfully.

Data: Reply URL

Triggers: Successful single logout.

OpenAM logs the following WebServicesSecurity messages.

UNSUPPORTED_TOKEN_TYPE

ID: WebServicesSecurity-1

Level: INFO

Description: Unsupported Token Type sent to STS for Security Token creation.

Data: Token Type sent by client to STS

Triggers: Invalid or unsupported token type sent by client to STS.

Actions: Check the Token Type sent by client to STS.

CREATED_SAML11_ASSERTION

ID: WebServicesSecurity-2

Level: INFO

Description: Successfully created SAML 1.1 assertion by STS.

Data: Assertion ID, Issuer of this SAML assertion, Service Provider for which this Assertion is created or applies to, Confirmation Method, Token Type, Key Type

Triggers: Valid parameters sent by client to STS to create SAML assetion.

CREATED_SAML20_ASSERTION

ID: WebServicesSecurity-3

Level: INFO

Description: Successfully created SAML 2.0 assertion by STS.

Data: Assertion ID, Issuer of this SAML assertion, Service Provider for which this Assertion is created or applies to, Confirmation Method, Token Type, Key Type

Triggers: Valid parameters sent by client to STS to create SAML assetion.

ERROR_SIGNING_SAML_ASSERTION

ID: WebServicesSecurity-4

Level: INFO

Description: Error during signing SAML assertion by STS.

Data: Actual Error message

Triggers: Problem in STS's Certificate or Private key.

Actions: Check the certificate of STS.; Check the Private Key of STS.

ERROR_CREATING_SAML11_ASSERTION

ID: WebServicesSecurity-5

Level: INFO

Description: Error during creation of SAML 1.1 Assertion by STS.

Data: Actual Error message

Triggers: Invalid parameters sent to create SAML 1.1 Assertion.

Actions: Check all the parameters sent to create SAML 1.1 Assertion.

ERROR_CREATING_SAML20_ASSERTION

ID: WebServicesSecurity-6

Level: INFO

Description: Error during creation of SAML 2.0 Assertion by STS.

Data: Actual Error message

Triggers: Invalid parameters sent to create SAML 2.0 Assertion.

Actions: Check all the parameters sent to create SAML 2.0 Assertion.

IDENTITY_SUBJECT_NAME

ID: WebServicesSecurity-7

Level: INFO

Description: Security token being created for this Identity.

Data: Subject or Identity of the token

ATTR_MAP_FOR_SP

ID: WebServicesSecurity-8

Level: INFO

Description: Security token being created with this Attribute Map for Service Provider.

Data: Attribute Map required by Service Provider

Triggers: Service Provider needs Attributes to be populated in Security token.

SUCCESS_VALIDATE_REQUEST

ID: WebServicesSecurity-9

Level: INFO

Description: Successfully validated the incoming SOAP request.

Data: Provider name to identify the STS service or WSP profile, Security Mechanism or authentication token sent by client

REQUEST_TO_BE_VALIDATED

ID: WebServicesSecurity-10

Level: FINE

Description: Incoming SOAP request to be validated.

Data: Complete SOAP request

RESPONSE_TO_BE_SECURED

ID: WebServicesSecurity-11

Level: FINE

Description: Outgoing SOAP response to be secured.

Data: Complete SOAP response

SUCCESS_SECURE_RESPONSE

ID: WebServicesSecurity-12

Level: INFO

Description: Successfully secured the outgoing SOAP response.

Data: Provider name to identify the STS service or WSP profile

REQUEST_TO_BE_SECURED

ID: WebServicesSecurity-13

Level: FINE

Description: Outgoing SOAP request to be secured.

Data: Complete SOAP request

SUCCESS_SECURE_REQUEST

ID: WebServicesSecurity-14

Level: INFO

Description: Successfully secured the outgoing SOAP request.

Data: Provider name to identify the STS client or WSC profile, Security Mechanism or authentication token sent by client

RESPONSE_TO_BE_VALIDATED

ID: WebServicesSecurity-15

Level: FINE

Description: Incoming SOAP response to be validated.

Data: Complete SOAP response

SUCCESS_VALIDATE_RESPONSE

ID: WebServicesSecurity-16

Level: INFO

Description: Successfully validated the incoming SOAP response.

Data: Provider name to identify the STS client or WSC profile

AUTHENTICATION_FAILED

ID: WebServicesSecurity-17

Level: INFO

Description: Authentication of the incoming SOAP request failed at server or WSP.

Data: Security Mechanism or Security token sent by client

Triggers: Invalid Security Mechanism or Security token sent by client.

Actions: Check Security Mechanism or Security token sent by client.

ERROR_PARSING_SOAP_HEADERS

ID: WebServicesSecurity-18

Level: INFO

Description: Error in parsing SOAP headers from incoming SOAP request.

Data: Actual error message

Triggers: Client has sent incorrect SOAP headers.

Actions: Check SOAP headers.

ERROR_ADDING_SECURITY_HEADER

ID: WebServicesSecurity-19

Level: INFO

Description: Error in adding Security header in outgoing SOAP request.

Data: Actual error message

Triggers: Error in adding namespaces or creating Security Header element.

Actions: Check namespaces and Secuirty Header.

SIGNATURE_VALIDATION_FAILED

ID: WebServicesSecurity-20

Level: INFO

Description: Signature validation failed in incoming SOAP request / response.

Data: Actual error message

Triggers: Error in signing request / response by client / server.

Actions: Check keystore and certificate used for signing.

UNABLE_TO_SIGN

ID: WebServicesSecurity-21

Level: INFO

Description: Unable to sign SOAP request or response.

Data: Actual error message

Triggers: Error in retrieving certificate from the keystore.

Actions: Check keystore configuration and certificate used for signing.; Check debug file for detailed info.

UNABLE_TO_ENCRYPT

ID: WebServicesSecurity-22

Level: INFO

Description: Unable to encrypt SOAP request or response.

Data: Actual error message

Triggers: Error in retrieving certificate from the keystore.

Actions: Check keystore configuration and certificate used for encryption.; Check debug file for detailed info.

UNABLE_TO_DECRYPT

ID: WebServicesSecurity-23

Level: INFO

Description: Unable to decrypt SOAP request or response.

Data: Actual error message

Triggers: Error in retrieving certificate from the keystore.

Actions: Check keystore configuration and certificate used for decryption.; Check debug file for detailed info.

SUCCESS_RETRIEVING_TOKEN_FROM_STS

ID: WebServicesSecurity-24

Level: INFO

Description: Successfully retrieved Security Token from STS service.

Data: Web Service Provider end point for which Security Token being generated, Security Token Service end point to which STS client talks to, Security Token Service MEX end point address, End user credential (if "null" then the Identity of the generated Security token is Web Service Client, else it is owned by Authenticated End user), Key Type, Token Type

Triggers: All the required input data parameters are correct.

ERROR_RETRIEVING_TOKEN_FROM_STS

ID: WebServicesSecurity-25

Level: INFO

Description: Error in retrieving Security Token from STS service.

Data: Actual error message

Triggers: Some or more required input data parameters are not correct.

Actions: Check all the required input data parameters.; Check debug file for detailed error.

ERROR_RETRIEVING_TOKEN_FROM_STS

ID: WebServicesSecurity-26

Level: SEVERE

Description: Error in retrieving Security Token from STS service.

Data: Actual error message

Triggers: Some or more required input data parameters are not correct.

Actions: Check all the required input data parameters.; Check debug file for detailed error.

ERROR_CREATING_SAML11_ASSERTION

ID: WebServicesSecurity-27

Level: SEVERE

Description: Error during creation of SAML 1.1 Assertion by STS.

Data: Actual Error message

Triggers: Invalid parameters sent to create SAML 1.1 Assertion.

Actions: Check all the parameters sent to create SAML 1.1 Assertion.; Check debug file for detailed error.

ERROR_CREATING_SAML20_ASSERTION

ID: WebServicesSecurity-28

Level: SEVERE

Description: Error during creation of SAML 2.0 Assertion by STS.

Data: Actual Error message

Triggers: Invalid parameters sent to create SAML 2.0 Assertion.

Actions: Check all the parameters sent to create SAML 2.0 Assertion.; Check debug file for detailed error.

OpenAM logs the following AUTHENTICATION messages.

LOGIN_SUCCESS

ID: AUTHENTICATION-100

Level: INFO

Description: Authentication is Successful

Data: message, no session

Triggers: User authenticated with valid credentials

LOGIN_SUCCESS_USER

ID: AUTHENTICATION-101

Level: INFO

Description: User based authentication is successful

Data: message, authentication type, user name, no session

Triggers: User authenticated with valid credentials

LOGIN_SUCCESS_ROLE

ID: AUTHENTICATION-102

Level: INFO

Description: Role based authentication is successful

Data: message, authentication type, role name, no session

Triggers: User belonging to role authenticated with valid credentials

LOGIN_SUCCESS_SERVICE

ID: AUTHENTICATION-103

Level: INFO

Description: Service based authentication is successful

Data: message, authentication type, service name, no session

Triggers: User authenticated with valid credentials to a configured service under realm

LOGIN_SUCCESS_LEVEL

ID: AUTHENTICATION-104

Level: INFO

Description: Authentication level based authentication is successful

Data: message, authentication type, authentication level value, no session

Triggers: User authenticated with valid credentials to one or more authentication modules having authentication level value greater than or equal to specified authentication level

LOGIN_SUCCESS_MODULE_INSTANCE

ID: AUTHENTICATION-105

Level: INFO

Description: Module based authentication is successful

Data: message, authentication type, module name, no session

Triggers: User authenticated with valid credentials to authentication module under realm

LOGIN_FAILED

ID: AUTHENTICATION-200

Level: INFO

Description: Authentication Failed

Data: error message

Triggers: Incorrect/invalid credentials presented; User locked out/not active

Actions: Enter correct/valid credentials to required authentication module

LOGIN_FAILED_INVALIDPASSWORD

ID: AUTHENTICATION-201

Level: INFO

Description: Authentication Failed

Data: error message

Triggers: Invalid credentials entered.

Actions: Enter the correct password.

LOGIN_FAILED_NOCONFIG

ID: AUTHENTICATION-202

Level: INFO

Description: Authentication Failed

Data: error message

Triggers: Named Configuration (Auth Chain) does not exist.

Actions: Create and configure a named config for this org.

LOGIN_FAILED_NOUSERPROFILE

ID: AUTHENTICATION-203

Level: INFO

Description: Authentication Failed

Data: error message

Triggers: No user profile found for this user.

Actions: User does not exist in the datastore plugin configured and hence configure the datastore plugin for this realm/org correctly.

LOGIN_FAILED_USERINACTIVE

ID: AUTHENTICATION-204

Level: INFO

Description: Authentication Failed

Data: error message

Triggers: This user is not active.

Actions: Activate the user.

LOGIN_FAILED_LOCKEDOUT

ID: AUTHENTICATION-205

Level: INFO

Description: Authentication Failed

Data: error message

Triggers: Max number of failure attempts exceeded. User is Locked out.

Actions: Contact system administrator.

LOGIN_FAILED_ACCOUNTEXPIRED

ID: AUTHENTICATION-206

Level: INFO

Description: Authentication Failed

Data: error message

Triggers: User account has expired.

Actions: Contact system administrator.

LOGIN_FAILED_LOGINTIMEOUT

ID: AUTHENTICATION-207

Level: INFO

Description: Authentication Failed

Data: error message

Triggers: Login timed out.

Actions: Try to login again.

LOGIN_FAILED_MODULEDENIED

ID: AUTHENTICATION-208

Level: INFO

Description: Authentication Failed

Data: error message

Triggers: Authentication module is denied.

Actions: Configure this module or use some other module.

LOGIN_FAILED_MAXSESSIONREACHED

ID: AUTHENTICATION-209

Level: INFO

Description: Authentication Failed

Data: error message

Triggers: Limit for maximum number of allowed session has been reached.

Actions: Logout of a session or increase the limit.

LOGIN_FAILED_INVALIDDOMAIN

ID: AUTHENTICATION-210

Level: INFO

Description: Authentication Failed

Data: error message

Triggers: Org/Realm does not exists.

Actions: Use a valid Org/Realm.

LOGIN_FAILED_ORGINACTIVE

ID: AUTHENTICATION-211

Level: INFO

Description: Authentication Failed

Data: error message

Triggers: Org/Realm is not active.

Actions: Activate the Org/Realm.

LOGIN_FAILED_SESSIONCREATEERROR

ID: AUTHENTICATION-212

Level: INFO

Description: Authentication Failed

Data: error message

Triggers: Cannot create a session.

Actions: Ensure that session service is configured and maxsession is not reached.

LOGIN_FAILED_USER

ID: AUTHENTICATION-213

Level: INFO

Description: User based authentication failed

Data: error message, authentication type, user name

Triggers: No authentication configuration (chain of one or more authentication modules) configured for user; Incorrect/invalid credentials presented; User locked out/not active

Actions: Configure authentication configuration (chain of one or more authentication modules) for user; Enter correct/valid credentials to required authentication module

LOGIN_FAILED_USER_INVALIDPASSWORD

ID: AUTHENTICATION-214

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, user name

Triggers: User based Auth. Invalid credentials entered.

Actions: Enter the correct password.

LOGIN_FAILED_USER_NOCONFIG

ID: AUTHENTICATION-215

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, user name

Triggers: Named Configuration (Auth Chain) does not exist for this user

Actions: Create and configure a named config for this user

LOGIN_FAILED_USER_NOUSERPROFILE

ID: AUTHENTICATION-216

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, user name

Triggers: User based Auth. No user profile found for this user.

Actions: User does not exist in the datastore plugin configured and hence configure the datastore plugin for this realm/org correctly.

LOGIN_FAILED_USER_USERINACTIVE

ID: AUTHENTICATION-217

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, user name

Triggers: User based Auth. This user is not active.

Actions: Activate the user.

LOGIN_FAILED_USER_LOCKEDOUT

ID: AUTHENTICATION-218

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, user name

Triggers: User based Auth. Max number of failure attempts exceeded. User is Locked out.

Actions: Contact system administrator.

LOGIN_FAILED_USER_ACCOUNTEXPIRED

ID: AUTHENTICATION-219

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, user name

Triggers: User based Auth. User account has expired.

Actions: Contact system administrator.

LOGIN_FAILED_USER_LOGINTIMEOUT

ID: AUTHENTICATION-220

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, user name

Triggers: User based Auth. Login timed out.

Actions: Try to login again.

LOGIN_FAILED_USER_MODULEDENIED

ID: AUTHENTICATION-221

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, user name

Triggers: User based Auth. Authentication module is denied.

Actions: Configure this module or use some other module.

LOGIN_FAILED_USER_MAXSESSIONREACHED

ID: AUTHENTICATION-222

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, user name

Triggers: User based auth. Limit for maximum number of allowed session has been reached.

Actions: Logout of a session or increase the limit.

LOGIN_FAILED_USER_INVALIDDOMAIN

ID: AUTHENTICATION-223

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, user name

Triggers: User based auth. Org/Realm does not exists.

Actions: Use a valid Org/Realm.

LOGIN_FAILED_USER_ORGINACTIVE

ID: AUTHENTICATION-224

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, user name

Triggers: User based auth. Org/Realm is not active.

Actions: Activate the Org/Realm.

LOGIN_FAILED_USER_SESSIONCREATEERROR

ID: AUTHENTICATION-225

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, user name

Triggers: User based auth. Cannot create a session.

Actions: Ensure that session service is configured and maxsession is not reached.

LOGIN_FAILED_ROLE

ID: AUTHENTICATION-226

Level: INFO

Description: Role based authentication failed

Data: error message, authentication type, role name

Triggers: No authentication configuration (chain of one or more authentication modules) configured for role; Incorrect/invalid credentials presented; User does not belong to this role; User locked out/not active

Actions: Configure authentication configuration (chain of one or more authentication modules) for role; Enter correct/valid credentials to required authentication module; Assign this role to the authenticating user

LOGIN_FAILED_ROLE_INVALIDPASSWORD

ID: AUTHENTICATION-227

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, role name

Triggers: Role based Auth. Invalid credentials entered.

Actions: Enter the correct password.

LOGIN_FAILED_ROLE_NOCONFIG

ID: AUTHENTICATION-228

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, role name

Triggers: Named Configuration (Auth Chain) does not exist for this role.

Actions: Create and configure a named config for this role.

LOGIN_FAILED_ROLE_NOUSERPROFILE

ID: AUTHENTICATION-229

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, role name

Triggers: Role based Auth. No user profile found for this user.

Actions: User does not exist in the datastore plugin configured and hence configure the datastore plugin for this realm/org correctly.

LOGIN_FAILED_ROLE_USERINACTIVE

ID: AUTHENTICATION-230

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, role name

Triggers: Role based Auth. This user is not active.

Actions: Activate the user.

LOGIN_FAILED_ROLE_LOCKEDOUT

ID: AUTHENTICATION-231

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, role name

Triggers: Role based Auth. Max number of failure attempts exceeded. User is Locked out.

Actions: Contact system administrator.

LOGIN_FAILED_ROLE_ACCOUNTEXPIRED

ID: AUTHENTICATION-232

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, role name

Triggers: Role based Auth. User account has expired.

Actions: Contact system administrator.

LOGIN_FAILED_ROLE_LOGINTIMEOUT

ID: AUTHENTICATION-233

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, role name

Triggers: Role based Auth. Login timed out.

Actions: Try to login again.

LOGIN_FAILED_ROLE_MODULEDENIED

ID: AUTHENTICATION-234

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, role name

Triggers: Role based Auth. Authentication module is denied.

Actions: Configure this module or use some other module.

LOGIN_FAILED_ROLE_MAXSESSIONREACHED

ID: AUTHENTICATION-235

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, role name

Triggers: Role based auth. Limit for maximum number of allowed session has been reached.

Actions: Logout of a session or increase the limit.

LOGIN_FAILED_ROLE_INVALIDDOMAIN

ID: AUTHENTICATION-236

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, role name

Triggers: Role based auth. Org/Realm does not exists.

Actions: Use a valid Org/Realm.

LOGIN_FAILED_ROLE_ORGINACTIVE

ID: AUTHENTICATION-237

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, role name

Triggers: Role based auth. Org/Realm is not active.

Actions: Activate the Org/Realm.

LOGIN_FAILED_ROLE_SESSIONCREATEERROR

ID: AUTHENTICATION-238

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, role name

Triggers: Role based auth. Cannot create a session.

Actions: Ensure that session service is configured and maxsession is not reached.

LOGIN_FAILED_ROLE_USERNOTFOUND

ID: AUTHENTICATION-239

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, role name

Triggers: Role based auth. User does not belong to this role.

Actions: Add the user to this role.

LOGIN_FAILED_SERVICE

ID: AUTHENTICATION-240

Level: INFO

Description: Service based authentication failed

Data: error message, authentication type, service name

Triggers: No authentication configuration (chain of one or more authentication modules) configured for service; Incorrect/invalid credentials presented; User locked out/not active

Actions: Configure authentication configuration (chain of one or more authentication modules) for service; Enter correct/valid credentials to required authentication module

LOGIN_FAILED_SERVICE_INVALIDPASSWORD

ID: AUTHENTICATION-241

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, service name

Triggers: Service based Auth. Invalid credentials entered.

Actions: Enter the correct password.

LOGIN_FAILED_SERVICE_NOCONFIG

ID: AUTHENTICATION-242

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, service name

Triggers: Named Configuration (Auth Chain) does not exist with this service name.

Actions: Create and configure a named config.

LOGIN_FAILED_SERVICE_NOUSERPROFILE

ID: AUTHENTICATION-243

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, service name

Triggers: Service based Auth. No user profile found for this user.

Actions: User does not exist in the datastore plugin configured and hence configure the datastore plugin for this realm/org correctly.

LOGIN_FAILED_SERVICE_USERINACTIVE

ID: AUTHENTICATION-244

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, service name

Triggers: Service based Auth. This user is not active.

Actions: Activate the user.

LOGIN_FAILED_SERVICE_LOCKEDOUT

ID: AUTHENTICATION-245

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, service name

Triggers: Service based Auth. Max number of failure attempts exceeded. User is Locked out.

Actions: Contact system administrator.

LOGIN_FAILED_SERVICE_ACCOUNTEXPIRED

ID: AUTHENTICATION-246

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, service name

Triggers: Service based Auth. User account has expired.

Actions: Contact system administrator.

LOGIN_FAILED_SERVICE_LOGINTIMEOUT

ID: AUTHENTICATION-247

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, service name

Triggers: Service based Auth. Login timed out.

Actions: Try to login again.

LOGIN_FAILED_SERVICE_MODULEDENIED

ID: AUTHENTICATION-248

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, service name

Triggers: Service based Auth. Authentication module is denied.

Actions: Configure this module or use some other module.

LOGIN_FAILED_SERVICE_NOSERVICE

ID: AUTHENTICATION-249

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, service name

Triggers: Service based Auth. Service does not exist.

Actions: Please use only valid Service.

LOGIN_FAILED_SERVICE_MAXSESSIONREACHED

ID: AUTHENTICATION-250

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, service name

Triggers: Service based auth. Limit for maximum number of allowed session has been reached.

Actions: Logout of a session or increase the limit.

LOGIN_FAILED_SERVICE_INVALIDDOMAIN

ID: AUTHENTICATION-251

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, service name

Triggers: Service based auth. Org/Realm does not exists.

Actions: Use a valid Org/Realm.

LOGIN_FAILED_SERVICE_ORGINACTIVE

ID: AUTHENTICATION-252

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, service name

Triggers: Service based auth. Org/Realm is not active.

Actions: Activate the Org/Realm.

LOGIN_FAILED_SERVICE_SESSIONCREATEERROR

ID: AUTHENTICATION-253

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, service name

Triggers: Service based auth. Cannot create a session.

Actions: Ensure that session service is configured and maxsession is not reached.

LOGIN_FAILED_LEVEL

ID: AUTHENTICATION-254

Level: INFO

Description: Authentication level based authentication failed

Data: error message, authentication type, authentication level value

Triggers: There are no authentication module(s) having authentication level value greater than or equal to specified authentication level; Incorrect/invalid credentials presented to one or more authentication modules having authentication level greater than or equal to specified authentication level; User locked out/not active

Actions: Configure one or more authentication modules having authentication level value greater than or equal to required authentication level; Enter correct/valid credentials to one or more authentication modules having authentication level greater than or equal to specified authentication level

LOGIN_FAILED_LEVEL_INVALIDPASSWORD

ID: AUTHENTICATION-255

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, authentication level value

Triggers: Level based Auth. Invalid credentials entered.

Actions: Enter the correct password.

LOGIN_FAILED_LEVEL_NOCONFIG

ID: AUTHENTICATION-256

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, authentication level value

Triggers: Level based Auth. No Auth Configuration available.

Actions: Create an auth configuration.

LOGIN_FAILED_LEVEL_NOUSERPROFILE

ID: AUTHENTICATION-257

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, authentication level value

Triggers: Level based Auth. No user profile found for this user.

Actions: User does not exist in the datastore plugin configured and hence configure the datastore plugin for this realm/org correctly.

LOGIN_FAILED_LEVEL_USERINACTIVE

ID: AUTHENTICATION-258

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, authentication level value

Triggers: Level based Auth. This user is not active.

Actions: Activate the user.

LOGIN_FAILED_LEVEL_LOCKEDOUT

ID: AUTHENTICATION-259

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, authentication level value

Triggers: Level based Auth. Max number of failure attempts exceeded. User is Locked out.

Actions: Contact system administrator.

LOGIN_FAILED_LEVEL_ACCOUNTEXPIRED

ID: AUTHENTICATION-260

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, authentication level value

Triggers: Level based Auth. User account has expired.

Actions: Contact system administrator.

LOGIN_FAILED_LEVEL_LOGINTIMEOUT

ID: AUTHENTICATION-261

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, authentication level value

Triggers: Level based Auth. Login timed out.

Actions: Try to login again.

LOGIN_FAILED_LEVEL_MODULEDENIED

ID: AUTHENTICATION-262

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, authentication level value

Triggers: Level based Auth. Authentication module is denied.

Actions: Configure this module or use some other module.

LOGIN_FAILED_LEVEL_INCORRECTLEVEL

ID: AUTHENTICATION-263

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, authentication level value

Triggers: Level based Auth. Invalid Authg Level.

Actions: Please specify valid auth level.

LOGIN_FAILED_LEVEL_MAXSESSIONREACHED

ID: AUTHENTICATION-264

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, authentication level value

Triggers: Level based auth. Limit for maximum number of allowed session has been reached.

Actions: Logout of a session or increase the limit.

LOGIN_FAILED_LEVEL_INVALIDDOMAIN

ID: AUTHENTICATION-265

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, authentication level value

Triggers: Level based auth. Org/Realm does not exists.

Actions: Use a valid Org/Realm.

LOGIN_FAILED_LEVEL_ORGINACTIVE

ID: AUTHENTICATION-266

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, authentication level value

Triggers: Level based auth. Org/Realm is not active.

Actions: Activate the Org/Realm.

LOGIN_FAILED_LEVEL_SESSIONCREATEERROR

ID: AUTHENTICATION-267

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, authentication level value

Triggers: Level based auth. Cannot create a session.

Actions: Ensure that session service is configured and maxsession is not reached.

LOGIN_FAILED_MODULE_INSTANCE

ID: AUTHENTICATION-268

Level: INFO

Description: Module based authentication failed

Data: error message, authentication type, module name

Triggers: Module is not registered/configured under realm; Incorrect/invalid credentials presented; User locked out/not active

Actions: Register/configure authentication module under realm; Enter correct/valid credentials to authentication module

LOGIN_FAILED_MODULE_INSTANCE_INVALIDPASSWORD

ID: AUTHENTICATION-269

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, module name

Triggers: Module based Auth. Invalid credentials entered.

Actions: Enter the correct password.

LOGIN_FAILED_MODULE_INSTANCE_NOUSERPROFILE

ID: AUTHENTICATION-270

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, module name

Triggers: Module based Auth. No user profile found for this user.

Actions: User does not exist in the datastore plugin configured and hence configure the datastore plugin for this realm/org correctly.

LOGIN_FAILED_MODULE_INSTANCE_USERINACTIVE

ID: AUTHENTICATION-271

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, module name

Triggers: Module based Auth. This user is not active.

Actions: Activate the user.

LOGIN_FAILED_MODULE_INSTANCE_LOCKEDOUT

ID: AUTHENTICATION-272

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, module name

Triggers: Module based Auth. Max number of failure attempts exceeded. User is Locked out.

Actions: Contact system administrator.

LOGIN_FAILED_MODULE_INSTANCE_ACCOUNTEXPIRED

ID: AUTHENTICATION-273

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, module name

Triggers: Module based Auth. User account has expired.

Actions: Contact system administrator.

LOGIN_FAILED_MODULE_INSTANCE_LOGINTIMEOUT

ID: AUTHENTICATION-274

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, module name

Triggers: Module based Auth. Login timed out.

Actions: Try to login again.

LOGIN_FAILED_MODULE_INSTANCE_MODULEDENIED

ID: AUTHENTICATION-275

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, module name

Triggers: Module based Auth. Authentication module is denied.

Actions: Configure this module or use some other module.

LOGIN_FAILED_MODULE_INSTANCE_MAXSESSIONREACHED

ID: AUTHENTICATION-276

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, module name

Triggers: Module based auth. Limit for maximum number of allowed session has been reached.

Actions: Logout of a session or increase the limit.

LOGIN_FAILED_MODULE_INSTANCE_INVALIDDOMAIN

ID: AUTHENTICATION-277

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, module name

Triggers: Module based auth. Org/Realm does not exists.

Actions: Use a valid Org/Realm.

LOGIN_FAILED_MODULE_INSTANCE_ORGINACTIVE

ID: AUTHENTICATION-278

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, module name

Triggers: Module based auth. Org/Realm is not active.

Actions: Activate the Org/Realm.

LOGIN_FAILED_MODULE_INSTANCE_SESSIONCREATEERROR

ID: AUTHENTICATION-279

Level: INFO

Description: Authentication Failed

Data: error message, authentication type, module name

Triggers: Module based auth. Cannot create a session.

Actions: Ensure that session service is configured and maxsession is not reached.

LOGOUT

ID: AUTHENTICATION-300

Level: INFO

Description: User logout is Successful

Data: message

Triggers: User logged out

LOGOUT_USER

ID: AUTHENTICATION-301

Level: INFO

Description: User logout is successful from user based authentication

Data: message, authentication type, user name

Triggers: User logged out

LOGOUT_ROLE

ID: AUTHENTICATION-302

Level: INFO

Description: User logout is successful from role based authentication

Data: message, authentication type, role name

Triggers: User belonging to this role logged out

LOGOUT_SERVICE

ID: AUTHENTICATION-303

Level: INFO

Description: User logout is successful from service based authentication

Data: message, authentication type, service name

Triggers: User logged out of a configured service under realm

LOGOUT_LEVEL

ID: AUTHENTICATION-304

Level: INFO

Description: User logout is successful from authentication level based authentication

Data: message, authentication type, authentication level value

Triggers: User logged out of one or more authentication modules having authentication level value greater than or equal to specified authentication level

LOGOUT_MODULE_INSTANCE

ID: AUTHENTICATION-305

Level: INFO

Description: User logout is successful from module based authentication

Data: message, authentication type, module name

Triggers: User logged out of authentication module under realm

CHANGE_USER_PASSWORD_FAILED

ID: AUTHENTICATION-306

Level: INFO

Description: Change user password failed

Data: error message

Triggers: Change user password in authentication screen due to directory server password policy.

Actions: Enter password which meets directory server password policy

CHANGE_USER_PASSWORD_SUCCEEDED

ID: AUTHENTICATION-307

Level: INFO

Description: Changing user password succeeded

Data: message

Triggers: Change user password in authentication screen due to directory server password policy.

CREATE_USER_PROFILE_FAILED

ID: AUTHENTICATION-308

Level: INFO

Description: Create user password failed

Data: error message, user name

Triggers: Create new user in Membership module

Actions: Make sure password entered meets directory server password policy

OpenAM logs the following AMCLI messages.

ATTEMPT_LOGIN

ID: AMCLI-1

Level: INFO

Description: Attempt to login to execute the commandline.

Data: user ID

Triggers: Run the Commandline tool.

SUCCEED_LOGIN

ID: AMCLI-2

Level: INFO

Description: Login to execute the commandline.

Data: user ID

Triggers: Run the Commandline tool.

FAILED_LOGIN

ID: AMCLI-3

Level: INFO

Description: Failed to login.

Data: user ID, error message

Triggers: Run the Commandline tool.

Actions: Check your user ID and password.; Look under debug file for more information.

ATTEMPT_LOAD_SCHEMA

ID: AMCLI-20

Level: INFO

Description: Attempt to load schema to data store.

Data: XML file name

Triggers: Load Schema through Commandline interface.

SUCCESS_LOAD_SCHEMA

ID: AMCLI-21

Level: INFO

Description: Schema is loaded to data store.

Data: XML file name

Triggers: Load Schema through Commandline interface.

FAILED_LOAD_SCHEMA

ID: AMCLI-22

Level: SEVERE

Description: Schema is not loaded to data store.

Data: XML file name, error message

Triggers: Load Schema through Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_DELETE_SERVICE

ID: AMCLI-30

Level: INFO

Description: Attempt to delete service from data store.

Data: service name

Triggers: Delete Service through Commandline interface.

SUCCESS_DELETE_SERVICE

ID: AMCLI-31

Level: INFO

Description: Deleted service from data store.

Data: service name

Triggers: Delete Service through Commandline interface.

FAILED_DELETE_SERVICE

ID: AMCLI-32

Level: SEVERE

Description: Schema is not loaded to data store.

Data: service name, error message

Triggers: Delete Service Schema through Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_ADD_ATTRIBUTE_SCHEMA

ID: AMCLI-40

Level: INFO

Description: Attempt to attribute schema to an existing service.

Data: service name, schema type, XML file name

Triggers: Add attribute schema through Commandline interface.

SUCCESS_ADD_ATTRIBUTE_SCHEMA

ID: AMCLI-41

Level: INFO

Description: Added attribute schema to existing service.

Data: service name, schema type, XML file name

Triggers: Add attribute schema through Commandline interface.

FAILED_ADD_ATTRIBUTE_SCHEMA

ID: AMCLI-42

Level: SEVERE

Description: Attribute schema is not added to existing service.

Data: service name, schema type, XML file name, error message

Triggers: Add attribute schema through Commandline interface.

Actions: Check the service name, schema type and XML file.; Look under debug file for more information.

ATTEMPT_ADD_RESOURCE_BUNDLE

ID: AMCLI-50

Level: INFO

Description: Attempt to add resource bundle to data store.

Data: resource bundle name, file name, locale

Triggers: Add Resource Bundle through Commandline interface.

SUCCEED_ADD_RESOURCE_BUNDLE

ID: AMCLI-51

Level: INFO

Description: Resource bundle is added to data store.

Data: resource bundle name, file name, locale

Triggers: Add Resource Bundle through Commandline interface.

FAILED_ADD_RESOURCE_BUNDLE

ID: AMCLI-52

Level: SEVERE

Description: Failed to add resource bundle to data store.

Data: resource bundle name, file name, locale, error message

Triggers: SDK for adding resource bundle failed.

Actions: Look under debug file for more information.

ATTEMPT_GET_RESOURCE_BUNDLE

ID: AMCLI-60

Level: INFO

Description: Attempt to get resource bundle from data store.

Data: resource bundle name, locale

Triggers: Get Resource Bundle through Commandline interface.

SUCCEED_GET_RESOURCE_BUNDLE

ID: AMCLI-61

Level: INFO

Description: Resource bundle retrieved from data store.

Data: resource bundle name, locale

Triggers: Get Resource Bundle through Commandline interface.

FAILED_GET_RESOURCE_BUNDLE

ID: AMCLI-62

Level: SEVERE

Description: Failed to get resource bundle from data store.

Data: resource bundle name, locale, error message

Triggers: SDK for getting resource bundle failed.

Actions: Look under debug file for more information.

ATTEMPT_DELETE_RESOURCE_BUNDLE

ID: AMCLI-70

Level: INFO

Description: Attempt to delete resource bundle from data store.

Data: resource bundle name, locale

Triggers: Delete Resource Bundle through Commandline interface.

SUCCEED_DELETE_RESOURCE_BUNDLE

ID: AMCLI-71

Level: INFO

Description: Resource bundle deleted from data store.

Data: resource bundle name, locale

Triggers: Delete Resource Bundle through Commandline interface.

FAILED_DELETE_RESOURCE_BUNDLE

ID: AMCLI-72

Level: SEVERE

Description: Failed to delete resource bundle from data store.

Data: resource bundle name, locale, error message

Triggers: SDK for deleting resource bundle failed.

Actions: Look under debug file for more information.

ATTEMPT_SESSION_DESTROY

ID: AMCLI-100

Level: INFO

Description: Attempt to destroy Session destroyed

Data: name of user

Triggers: Administrator invalidates session via Commandline interface.

SUCCEED_SESSION_DESTROY

ID: AMCLI-101

Level: INFO

Description: Session destroyed

Data: name of user

Triggers: Administrator invalidates session via Commandline interface.

FAILED_SESSION_DESTROY

ID: AMCLI-102

Level: SEVERE

Description: Failed to destroy session

Data: name of user, error message

Triggers: Session cannot be destroyed.

Actions: Look under debug file for more information.

ATTEMPT_MIGRATION_ENTRY

ID: AMCLI-1000

Level: INFO

Description: Attempt to migration organization to realm/

Data: distinguished name of organization

Triggers: Migration Commandline interface.

SUCCEED_MIGRATION_ENTRY

ID: AMCLI-1001

Level: INFO

Description: Migration completed.

Data: distinguished name of organization

Triggers: Migration Commandline interface.

ATTEMPT_DELETE_REALM

ID: AMCLI-2000

Level: INFO

Description: Attempt to delete realm/

Data: name of realm, recursive

Triggers: Delete realm command through Commandline interface.

SUCCEED_DELETE_REALM

ID: AMCLI-2001

Level: INFO

Description: Realm deleted.

Data: name of realm, recursive

Triggers: Delete realm command through Commandline interface.

FAILED_DELETE_REALM

ID: AMCLI-2002

Level: INFO

Description: Failed to delete realm.

Data: name of realm, recursive, error message

Triggers: Delete realm command through Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_CREATE_REALM

ID: AMCLI-2010

Level: INFO

Description: Attempt to create realm/

Data: name of realm

Triggers: Create realm command through Commandline interface.

SUCCEED_CREATE_REALM

ID: AMCLI-2011

Level: INFO

Description: Realm created.

Data: name of realm

Triggers: Create realm command through Commandline interface.

FAILED_CREATE_REALM

ID: AMCLI-2012

Level: INFO

Description: Failed to create realm.

Data: name of realm, error message

Triggers: Create realm command through Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_SEARCH_REALM

ID: AMCLI-3020

Level: INFO

Description: Attempt to search for realms by name.

Data: name of realm, search pattern, recursive

Triggers: Search realms command through Commandline interface.

SUCCEED_SEARCH_REALM

ID: AMCLI-3021

Level: INFO

Description: Completed searching for realms.

Data: name of realm, search pattern, recursive

Triggers: Search realms command through Commandline interface.

FAILED_SEARCH_REALM

ID: AMCLI-3022

Level: INFO

Description: Search for realms failed.

Data: name of realm, search pattern, recursive, error message

Triggers: Search realms command through Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_GET_ASSIGNABLE_SERVICES_OF_REALM

ID: AMCLI-2020

Level: INFO

Description: Attempt to get assignable services of realm.

Data: name of realm

Triggers: Execute get assignable services of realm Commandline interface.

SUCCEED_GET_ASSIGNABLE_SERVICES_OF_REALM

ID: AMCLI-2021

Level: INFO

Description: Assignable services command is serviced.

Data: name of realm

Triggers: Execute get assignable services of realm Commandline interface.

FAILED_GET_ASSIGNABLE_SERVICES_OF_REALM

ID: AMCLI-2022

Level: INFO

Description: Unable to get assignable services of realm.

Data: name of realm, error message

Triggers: Execute get assignable services of realm Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_GET_ASSIGNED_SERVICES_OF_REALM

ID: AMCLI-2030

Level: INFO

Description: Attempt to get services assigned to a realm.

Data: name of realm, include mandatory services

Triggers: Execute get services assigned to realm Commandline interface.

SUCCEED_GET_ASSIGNED_SERVICES_OF_REALM

ID: AMCLI-2031

Level: INFO

Description: Assignable services command is serviced.

Data: name of realm, include mandatory services

Triggers: Execute get services assigned to realm Commandline interface.

FAILED_GET_ASSIGNED_SERVICES_OF_REALM

ID: AMCLI-2032

Level: INFO

Description: Unable to get services assigned to realm.

Data: name of realm, include mandatory services, error message

Triggers: Execute get services assigned to realm Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_ASSIGN_SERVICE_TO_REALM

ID: AMCLI-2040

Level: INFO

Description: Attempt to assign service to a realm.

Data: name of realm, name of service

Triggers: Execute assign service to realm Commandline interface.

SUCCEED_ASSIGN_SERVICE_TO_REALM

ID: AMCLI-2041

Level: INFO

Description: Service is assigned to realm.

Data: name of realm, name of service

Triggers: Execute assign service to realm Commandline interface.

FAILED_ASSIGN_SERVICE_TO_REALM

ID: AMCLI-2042

Level: INFO

Description: Unable to assign service to realm.

Data: name of realm, name of service, error message

Triggers: Execute assign service to realm Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_UNASSIGN_SERVICE_FROM_REALM

ID: AMCLI-2050

Level: INFO

Description: Attempt to unassign service from a realm.

Data: name of realm, name of service

Triggers: Execute unassign service from realm Commandline interface.

SUCCEED_UNASSIGN_SERVICE_FROM_REALM

ID: AMCLI-2051

Level: INFO

Description: Service is unassigned from realm.

Data: name of realm, name of service

Triggers: Execute unassign service from realm Commandline interface.

FAILED_UNASSIGN_SERVICE_FROM_REALM

ID: AMCLI-2052

Level: INFO

Description: Unable to unassign service from realm.

Data: name of realm, name of service, error message

Triggers: Execute unassign service from realm Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_GET_REALM_SERVICE_ATTR_VALUES

ID: AMCLI-2060

Level: INFO

Description: Attempt to get service attribute values from a realm.

Data: name of realm, name of service

Triggers: Execute get service attribute values from realm Commandline interface.

SUCCEED_GET_REALM_SERVICE_ATTR_VALUES

ID: AMCLI-2061

Level: INFO

Description: Service attribute values of realm is returneed.

Data: name of realm, name of service

Triggers: Execute get service attribute values from realm Commandline interface.

FAILED_GET_REALM_SERVICE_ATTR_VALUES

ID: AMCLI-2062

Level: INFO

Description: Unable to get service attribute values of realm.

Data: name of realm, name of service, error message

Triggers: Execute get service attribute values from realm Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_REMOVE_REALM_ATTRIBUTE

ID: AMCLI-2070

Level: INFO

Description: Attempt to remove attribute from a realm.

Data: name of realm, name of service, name of attribute

Triggers: Execute remove attribute from realm Commandline interface.

SUCCEED_REMOVE_REALM_ATTRIBUTE

ID: AMCLI-2071

Level: INFO

Description: Attribute of realm is removed.

Data: name of realm, name of service, name of attribute

Triggers: Execute remove attribute from realm Commandline interface.

FAILED_REMOVE_REALM_ATTRIBUTE

ID: AMCLI-2072

Level: INFO

Description: Unable to remove attribute from realm.

Data: name of realm, name of service, name of attribute, error message

Triggers: Execute remove attribute from realm Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_MODIFY_SERVICE_REALM

ID: AMCLI-2080

Level: INFO

Description: Attempt to modify service of realm.

Data: name of realm, name of service

Triggers: Execute modify service of realm Commandline interface.

SUCCEED_MODIFY_SERVICE_REALM

ID: AMCLI-2081

Level: INFO

Description: Attribute of realm is modified.

Data: name of realm, name of service

Triggers: Execute modify service of realm Commandline interface.

FAILED_MODIFY_SERVICE_REALM

ID: AMCLI-2082

Level: INFO

Description: Unable to modify service of realm.

Data: name of realm, name of service, error message

Triggers: Execute modify service of realm Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_ADD_ATTR_VALUES_REALM

ID: AMCLI-2090

Level: INFO

Description: Attempt to add attribute value to realm.

Data: name of realm, name of service, name of attribute

Triggers: Execute add attribute values to realm Commandline interface.

SUCCEED_ADD_ATTR_VALUES_REALM

ID: AMCLI-2091

Level: INFO

Description: Attribute values is added to realm.

Data: name of realm, name of service, name of attribute

Triggers: Execute add attribute values to realm Commandline interface.

FAILED_ADD_ATTR_VALUES_REALM

ID: AMCLI-2092

Level: INFO

Description: Unable to add attribute values to realm.

Data: name of realm, name of service, name of attribute, error message

Triggers: Execute add attribute values to realm Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_SET_ATTR_VALUES_REALM

ID: AMCLI-2100

Level: INFO

Description: Attempt to set attribute value to realm.

Data: name of realm, name of service

Triggers: Execute set attribute values to realm Commandline interface.

SUCCEED_SET_ATTR_VALUES_REALM

ID: AMCLI-2101

Level: INFO

Description: Attribute values is set to realm.

Data: name of realm, name of service

Triggers: Execute set attribute values to realm Commandline interface.

FAILED_SET_ATTR_VALUES_REALM

ID: AMCLI-2102

Level: INFO

Description: Unable to set attribute values to realm.

Data: name of realm, name of service, error message

Triggers: Execute set attribute values to realm Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_REMOVE_SCHEMA_ATTR_DEFAULTS

ID: AMCLI-2110

Level: INFO

Description: Attempt to remove schema attribute defaults.

Data: name of service, schema type, name of sub schema, name of attribute

Triggers: Execute remove schema attribute defaults Commandline interface.

SUCCEED_REMOVE_SCHEMA_ATTR_DEFAULTS

ID: AMCLI-2111

Level: INFO

Description: Schema attribute defaults is removed.

Data: name of service, schema type, name of sub schema, name of attribute

Triggers: Execute remove schema attribute defaults Commandline interface.

FAILED_REMOVE_SCHEMA_ATTR_DEFAULTS

ID: AMCLI-2112

Level: INFO

Description: Unable to remove schema attribute defaults.

Data: name of service, schema type, name of sub schema, name of attribute, error message

Triggers: Execute remove schema attribute defaults Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_ADD_SCHEMA_ATTR_DEFAULTS

ID: AMCLI-2120

Level: INFO

Description: Attempt to add schema attribute defaults.

Data: name of service, schema type, name of sub schema, name of attribute

Triggers: Execute add schema attribute defaults Commandline interface.

SUCCEED_ADD_SCHEMA_ATTR_DEFAULTS

ID: AMCLI-2121

Level: INFO

Description: Schema attribute defaults is added.

Data: name of service, schema type, name of sub schema, name of attribute

Triggers: Execute add schema attribute defaults Commandline interface.

FAILED_ADD_SCHEMA_ATTR_DEFAULTS

ID: AMCLI-2122

Level: INFO

Description: Unable to add schema attribute defaults.

Data: name of service, schema type, name of sub schema, name of attribute, error message

Triggers: Execute add schema attribute defaults Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_GET_SCHEMA_ATTR_DEFAULTS

ID: AMCLI-2130

Level: INFO

Description: Attempt to get schema attribute defaults.

Data: name of service, schema type, name of sub schema

Triggers: Execute get schema attribute defaults Commandline interface.

SUCCEED_GET_SCHEMA_ATTR_DEFAULTS

ID: AMCLI-2131

Level: INFO

Description: Schema attribute defaults is returned.

Data: name of service, schema type, name of sub schema

Triggers: Execute get schema attribute defaults Commandline interface.

FAILED_GET_SCHEMA_ATTR_DEFAULTS

ID: AMCLI-2132

Level: INFO

Description: Unable to get schema attribute defaults.

Data: name of service, schema type, name of sub schema, error message

Triggers: Execute get schema attribute defaults Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_SET_SCHEMA_ATTR_DEFAULTS

ID: AMCLI-2140

Level: INFO

Description: Attempt to set schema attribute defaults.

Data: name of service, schema type, name of sub schema

Triggers: Execute set schema attribute defaults Commandline interface.

SUCCEED_SET_SCHEMA_ATTR_DEFAULTS

ID: AMCLI-2141

Level: INFO

Description: Schema attribute defaults is set.

Data: name of service, schema type, name of sub schema

Triggers: Execute set schema attribute defaults Commandline interface.

FAILED_SET_SCHEMA_ATTR_DEFAULTS

ID: AMCLI-2142

Level: INFO

Description: Unable to set schema attribute defaults.

Data: name of service, schema type, name of sub schema, error message

Triggers: Execute set schema attribute defaults Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_ADD_ATTRIBUTE_SCHEMA_CHOICE_VALUES

ID: AMCLI-2150

Level: INFO

Description: Attempt to add choice value to attribute schema.

Data: name of service, schema type, name of sub schema, name of attribute schema

Triggers: Execute add attribute schema choice values Commandline interface.

SUCCEED_ADD_ATTRIBUTE_SCHEMA_CHOICE_VALUES

ID: AMCLI-2151

Level: INFO

Description: Choice values are added.

Data: name of service, schema type, name of sub schema, name of attribute schema

Triggers: Execute add attribute schema choice values Commandline interface.

FAILED_ADD_ATTRIBUTE_SCHEMA_CHOICE_VALUES

ID: AMCLI-2152

Level: INFO

Description: Unable to add choice value to attribute schema.

Data: name of service, schema type, name of sub schema, name of attribute schema, error message

Triggers: Execute add attribute schema choice values Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_GET_ATTRIBUTE_SCHEMA_CHOICE_VALUES

ID: AMCLI-2155

Level: INFO

Description: Attempt to get choice value to attribute schema.

Data: name of service, schema type, name of sub schema, name of attribute schema

Triggers: Execute get attribute schema choice values Commandline interface.

SUCCEED_GET_ATTRIBUTE_SCHEMA_CHOICE_VALUES

ID: AMCLI-2156

Level: INFO

Description: Choice values are listed.

Data: name of service, schema type, name of sub schema, name of attribute schema

Triggers: Execute get attribute schema choice values Commandline interface.

FAILED_GET_ATTRIBUTE_SCHEMA_CHOICE_VALUES

ID: AMCLI-2157

Level: INFO

Description: Unable to get choice value to attribute schema.

Data: name of service, schema type, name of sub schema, name of attribute schema, error message

Triggers: Execute get attribute schema choice values Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_REMOVE_ATTRIBUTE_SCHEMA_CHOICE_VALUE

ID: AMCLI-2160

Level: INFO

Description: Attempt to remove choice value from attribute schema.

Data: name of service, schema type, name of sub schema, name of attribute schema

Triggers: Execute remove attribute schema choice values Commandline interface.

SUCCEED_REMOVE_ATTRIBUTE_SCHEMA_CHOICE_VALUE

ID: AMCLI-2161

Level: INFO

Description: Choice value is removed.

Data: name of service, schema type, name of sub schema, name of attribute schema

Triggers: Execute remove attribute schema choice values Commandline interface.

FAILED_REMOVE_ATTRIBUTE_SCHEMA_CHOICE_VALUE

ID: AMCLI-2162

Level: INFO

Description: Unable to remove choice value to attribute schema.

Data: name of service, schema type, name of sub schema, name of attribute schema, error message

Triggers: Execute remove attribute schema choice values Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_MODIFY_ATTRIBUTE_SCHEMA_TYPE

ID: AMCLI-2170

Level: INFO

Description: Attempt to modify attribute schema type.

Data: name of service, schema type, name of sub schema, name of attribute schema, attribute schema type

Triggers: Execute modify attribute schema type Commandline interface.

SUCCEED_MODIFY_ATTRIBUTE_SCHEMA_TYPE

ID: AMCLI-2171

Level: INFO

Description: Attribute schema type is modified.

Data: name of service, schema type, name of sub schema, name of attribute schema, attribute schema type

Triggers: Execute modify attribute schema type Commandline interface.

FAILED_MODIFY_ATTRIBUTE_SCHEMA_TYPE

ID: AMCLI-2172

Level: INFO

Description: Unable to modify attribute schema type.

Data: name of service, schema type, name of sub schema, name of attribute schema, attribute schema type, error message

Triggers: Execute modify attribute schema type Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_MODIFY_ATTRIBUTE_SCHEMA_UI_TYPE

ID: AMCLI-2180

Level: INFO

Description: Attempt to modify attribute schema UI type.

Data: name of service, schema type, name of sub schema, name of attribute schema, attribute schema UI type

Triggers: Execute modify attribute schema UI type Commandline interface.

SUCCEED_MODIFY_ATTRIBUTE_SCHEMA_UI_TYPE

ID: AMCLI-2181

Level: INFO

Description: Attribute schema UI type is modified.

Data: name of service, schema type, name of sub schema, name of attribute schema, attribute schema UI type

Triggers: Execute modify attribute schema UI type Commandline interface.

FAILED_MODIFY_ATTRIBUTE_SCHEMA_UI_TYPE

ID: AMCLI-2182

Level: INFO

Description: Unable to modify attribute schema UI type.

Data: name of service, schema type, name of sub schema, name of attribute schema, attribute schema UI type, error message

Triggers: Execute modify attribute schema UI type Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_MODIFY_ATTRIBUTE_SCHEMA_SYNTAX

ID: AMCLI-2190

Level: INFO

Description: Attempt to modify attribute schema syntax.

Data: name of service, schema type, name of sub schema, name of attribute schema, attribute schema syntax

Triggers: Execute modify attribute schema syntax Commandline interface.

SUCCEED_MODIFY_ATTRIBUTE_SCHEMA_SYNTAX

ID: AMCLI-2191

Level: INFO

Description: Attribute schema syntax is modified.

Data: name of service, schema type, name of sub schema, name of attribute schema, attribute schema syntax

Triggers: Execute modify attribute schema syntax Commandline interface.

FAILED_MODIFY_ATTRIBUTE_SCHEMA_SYNTAX

ID: AMCLI-2192

Level: INFO

Description: Unable to modify attribute schema syntax.

Data: name of service, schema type, name of sub schema, name of attribute schema, attribute schema syntax, error message

Triggers: Execute modify attribute schema syntax Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_MODIFY_ATTRIBUTE_SCHEMA_I18N_KEY

ID: AMCLI-2200

Level: INFO

Description: Attempt to modify attribute schema i18n Key.

Data: name of service, schema type, name of sub schema, name of attribute schema, attribute schema i18n Key

Triggers: Execute modify attribute schema i18n Key Commandline interface.

SUCCEED_MODIFY_ATTRIBUTE_SCHEMA_I18N_KEY

ID: AMCLI-2201

Level: INFO

Description: Attribute schema i18n Key is modified.

Data: name of service, schema type, name of sub schema, name of attribute schema, attribute schema i18n Key

Triggers: Execute modify attribute schema i18n Key Commandline interface.

FAILED_MODIFY_ATTRIBUTE_SCHEMA_I18N_KEY

ID: AMCLI-2202

Level: INFO

Description: Unable to modify attribute schema i18n Key.

Data: name of service, schema type, name of sub schema, name of attribute schema, attribute schema i18n Key, error message

Triggers: Execute modify attribute schema i18n Key Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_MODIFY_ATTRIBUTE_SCHEMA_PROPERTIES_VIEW_BEAN_URL

ID: AMCLI-2210

Level: INFO

Description: Attempt to modify attribute schema properties view bean URL.

Data: name of service, schema type, name of sub schema, name of attribute schema, attribute schema properties view bean URL

Triggers: Execute modify attribute schema properties view bean URL Commandline interface.

SUCCEED_MODIFY_ATTRIBUTE_SCHEMA_PROPERTIES_VIEW_BEAN_URL

ID: AMCLI-2211

Level: INFO

Description: Attribute schema properties view bean URL is modified.

Data: name of service, schema type, name of sub schema, name of attribute schema, attribute schema properties view bean URL

Triggers: Execute modify attribute schema properties view bean URL Commandline interface.

FAILED_MODIFY_ATTRIBUTE_SCHEMA_PROPERTIES_VIEW_BEAN_URL

ID: AMCLI-2212

Level: INFO

Description: Unable to modify attribute schema properties view bean URL.

Data: name of service, schema type, name of sub schema, name of attribute schema, attribute schema properties view bean URL, error message

Triggers: Execute modify attribute schema properties view bean URL Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_MODIFY_ATTRIBUTE_SCHEMA_ANY

ID: AMCLI-2220

Level: INFO

Description: Attempt to modify attribute schema any value.

Data: name of service, schema type, name of sub schema, name of attribute schema, attribute schema any

Triggers: Execute modify attribute schema any Commandline interface.

SUCCEED_MODIFY_ATTRIBUTE_SCHEMA_ANY

ID: AMCLI-2221

Level: INFO

Description: Attribute schema any value is modified.

Data: name of service, schema type, name of sub schema, name of attribute schema, attribute schema any

Triggers: Execute modify attribute schema any Commandline interface.

FAILED_MODIFY_ATTRIBUTE_SCHEMA_ANY

ID: AMCLI-2222

Level: INFO

Description: Unable to modify attribute schema any value.

Data: name of service, schema type, name of sub schema, name of attribute schema, attribute schema any, error message

Triggers: Execute modify attribute schema any Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_REMOVE_ATTRIBUTE_SCHEMA_DEFAULT_VALUE

ID: AMCLI-2230

Level: INFO

Description: Attempt to remove attribute schema default value.

Data: name of service, schema type, name of sub schema, name of attribute schema, default value to be removed

Triggers: Execute remove attribute schema default values Commandline interface.

SUCCEED_REMOVE_ATTRIBUTE_SCHEMA_DEFAULT_VALUE

ID: AMCLI-2231

Level: INFO

Description: Attribute schema default value is removed.

Data: name of service, schema type, name of sub schema, name of attribute schema, default value to be removed

Triggers: Execute remove attribute schema default values Commandline interface.

FAILED_REMOVE_ATTRIBUTE_SCHEMA_DEFAULT_VALUE

ID: AMCLI-2232

Level: INFO

Description: Unable to remove attribute schema default value.

Data: name of service, schema type, name of sub schema, name of attribute schema, default value to be removed, error message

Triggers: Execute remove attribute schema default values Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_SET_ATTRIBUTE_SCHEMA_VALIDATOR

ID: AMCLI-2240

Level: INFO

Description: Attempt to set attribute schema validator.

Data: name of service, schema type, name of sub schema, name of attribute schema, validator

Triggers: Execute set attribute schema validator Commandline interface.

SUCCEED_SET_ATTRIBUTE_SCHEMA_VALIDATOR

ID: AMCLI-2241

Level: INFO

Description: Attribute schema validator is set.

Data: name of service, schema type, name of sub schema, name of attribute schema, validator

Triggers: Execute set attribute schema validator Commandline interface.

FAILED_SET_ATTRIBUTE_SCHEMA_VALIDATOR

ID: AMCLI-2242

Level: INFO

Description: Unable to set attribute schema validator.

Data: name of service, schema type, name of sub schema, name of attribute schema, validator, error message

Triggers: Execute set attribute schema validator Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_SET_ATTRIBUTE_SCHEMA_START_RANGE

ID: AMCLI-2250

Level: INFO

Description: Attempt to set attribute schema start range.

Data: name of service, schema type, name of sub schema, name of attribute schema, start range

Triggers: Execute set attribute schema start range Commandline interface.

SUCCEED_SET_ATTRIBUTE_SCHEMA_START_RANGE

ID: AMCLI-2251

Level: INFO

Description: Attribute schema start range is set.

Data: name of service, schema type, name of sub schema, name of attribute schema, start range

Triggers: Execute set attribute schema start range Commandline interface.

FAILED_SET_ATTRIBUTE_SCHEMA_START_RANGE

ID: AMCLI-2252

Level: INFO

Description: Unable to set attribute schema start range.

Data: name of service, schema type, name of sub schema, name of attribute schema, start range, error message

Triggers: Execute set attribute schema start range Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_SET_ATTRIBUTE_SCHEMA_END_RANGE

ID: AMCLI-2250

Level: INFO

Description: Attempt to set attribute schema end range.

Data: name of service, schema type, name of sub schema, name of attribute schema, end range

Triggers: Execute set attribute schema end range Commandline interface.

SUCCEED_SET_ATTRIBUTE_SCHEMA_END_RANGE

ID: AMCLI-2251

Level: INFO

Description: Attribute schema end range is set.

Data: name of service, schema type, name of sub schema, name of attribute schema, end range

Triggers: Execute set attribute schema end range Commandline interface.

FAILED_SET_ATTRIBUTE_SCHEMA_END_RANGE

ID: AMCLI-2252

Level: INFO

Description: Unable to set attribute schema end range.

Data: name of service, schema type, name of sub schema, name of attribute schema, end range, error message

Triggers: Execute set attribute schema end range Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_SET_SERVICE_SCHEMA_I18N_KEY

ID: AMCLI-2260

Level: INFO

Description: Attempt to set service schema i18n key.

Data: name of service, i18n key

Triggers: Execute set service schema i18n key Commandline interface.

SUCCEED_SET_SERVICE_SCHEMA_I18N_KEY

ID: AMCLI-2261

Level: INFO

Description: Service schema i18n key is set.

Data: name of service, i18n key

Triggers: Execute set service schema i18n key Commandline interface.

FAILED_SET_SERVICE_SCHEMA_I18N_KEY

ID: AMCLI-2262

Level: INFO

Description: Unable to set service schema i18n key.

Data: name of service, i18n key, error message

Triggers: Execute set service schema i18n key Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_SET_SERVICE_SCHEMA_PROPERTIES_VIEW_BEAN_URL

ID: AMCLI-2270

Level: INFO

Description: Attempt to set service schema properties view bean URL.

Data: name of service, properties view bean URL

Triggers: Execute set service schema properties view bean URL Commandline interface.

SUCCEED_SET_SERVICE_SCHEMA_PROPERTIES_VIEW_BEAN_URL

ID: AMCLI-2271

Level: INFO

Description: Service schema properties view bean URL is set.

Data: name of service, properties view bean URL

Triggers: Execute set service schema properties view bean URL Commandline interface.

FAILED_SET_SERVICE_SCHEMA_PROPERTIES_VIEW_BEAN_URL

ID: AMCLI-2272

Level: INFO

Description: Unable to set service schema properties view bean URL.

Data: name of service, properties view bean URL, error message

Triggers: Execute set service schema properties view bean URL Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_SET_SERVICE_REVISION_NUMBER

ID: AMCLI-2280

Level: INFO

Description: Attempt to set service revision number.

Data: name of service, revision number

Triggers: Execute set service revision number Commandline interface.

SUCCEED_SET_SERVICE_REVISION_NUMBER

ID: AMCLI-2281

Level: INFO

Description: Service revision number is set.

Data: name of service, revision number

Triggers: Execute set service revision number Commandline interface.

FAILED_SET_SERVICE_REVISION_NUMBER

ID: AMCLI-2282

Level: INFO

Description: Unable to set service revision number.

Data: name of service, revision number, error message

Triggers: Execute set service revision number Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_GET_SERVICE_REVISION_NUMBER

ID: AMCLI-2290

Level: INFO

Description: Attempt to get service revision number.

Data: name of service

Triggers: Execute get service revision number Commandline interface.

SUCCEED_GET_SERVICE_REVISION_NUMBER

ID: AMCLI-2291

Level: INFO

Description: Service revision number is returned.

Data: name of service

Triggers: Execute get service revision number Commandline interface.

FAILED_GET_SERVICE_REVISION_NUMBER

ID: AMCLI-2292

Level: INFO

Description: Unable to get service revision number.

Data: name of service, error message

Triggers: Execute get service revision number Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_REMOVE_ATTRIBUTE_SCHEMA

ID: AMCLI-2300

Level: INFO

Description: Attempt to remove attribute schema.

Data: name of service, schema type, name of sub schema, name of attribute schema

Triggers: Execute remove attribute schema Commandline interface.

SUCCEED_REMOVE_ATTRIBUTE_SCHEMA

ID: AMCLI-2301

Level: INFO

Description: Attribute schema is removed.

Data: name of service, schema type, name of sub schema, name of attribute schema

Triggers: Execute remove attribute schema Commandline interface.

FAILED_REMOVE_ATTRIBUTE_SCHEMA

ID: AMCLI-2302

Level: INFO

Description: Unable to remove attribute schema.

Data: name of service, schema type, name of sub schema, name of attribute schema, error message

Triggers: Execute remove attribute schema Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_ADD_SUB_CONFIGURATION

ID: AMCLI-2310

Level: INFO

Description: Attempt to add sub configuration.

Data: name of sub configuration, name of service

Triggers: Execute add sub configuration Commandline interface.

SUCCEED_ADD_SUB_CONFIGURATION

ID: AMCLI-2311

Level: INFO

Description: Sub configuration is added.

Data: name of sub configuration, name of service

Triggers: Execute add sub configuration Commandline interface.

FAILED_ADD_SUB_CONFIGURATION

ID: AMCLI-2312

Level: INFO

Description: Unable to add sub configuration.

Data: name of sub configuration, name of service, error message

Triggers: Execute add sub configuration Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_ADD_SUB_CONFIGURATION_TO_REALM

ID: AMCLI-2320

Level: INFO

Description: Attempt to add sub configuration to realm.

Data: name of realm, name of sub configuration, name of service

Triggers: Execute add sub configuration Commandline interface.

SUCCEED_ADD_SUB_CONFIGURATION_TO_REALM

ID: AMCLI-2321

Level: INFO

Description: Sub configuration is added to realm.

Data: name of realm, name of sub configuration, name of service

Triggers: Execute add sub configuration Commandline interface.

FAILED_ADD_SUB_CONFIGURATION_TO_REALM

ID: AMCLI-2322

Level: INFO

Description: Unable to add sub configuration.

Data: name of realm, name of sub configuration, name of service, error message

Triggers: Execute add sub configuration Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_DELETE_SUB_CONFIGURATION

ID: AMCLI-2330

Level: INFO

Description: Attempt to delete sub configuration.

Data: name of sub configuration, name of service

Triggers: Execute delete sub configuration Commandline interface.

SUCCEED_DELETE_SUB_CONFIGURATION

ID: AMCLI-2331

Level: INFO

Description: Sub configuration is deleted.

Data: name of sub configuration, name of service

Triggers: Execute delete sub configuration Commandline interface.

FAILED_ADELETE_SUB_CONFIGURATION

ID: AMCLI-2332

Level: INFO

Description: Unable to delete sub configuration.

Data: name of sub configuration, name of service, error message

Triggers: Execute delete sub configuration Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_DELETE_SUB_CONFIGURATION_TO_REALM

ID: AMCLI-2340

Level: INFO

Description: Attempt to delete sub configuration from realm.

Data: name of realm, name of sub configuration, name of service

Triggers: Execute delete sub configuration Commandline interface.

SUCCEED_DELETE_SUB_CONFIGURATION_TO_REALM

ID: AMCLI-2341

Level: INFO

Description: Sub configuration is deleted from realm.

Data: name of realm, name of sub configuration, name of service

Triggers: Execute delete sub configuration Commandline interface.

FAILED_DELETE_SUB_CONFIGURATIONT_TO_REALM

ID: AMCLI-2342

Level: INFO

Description: Unable to delete sub configuration.

Data: name of realm, name of sub configuration, name of service, error message

Triggers: Execute delete sub configuration Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_ADD_SUB_SCHEMA

ID: AMCLI-2350

Level: INFO

Description: Attempt to add sub schema.

Data: name of service, schema type, name of sub schema

Triggers: Execute add sub schema Commandline interface.

SUCCEED_ADD_SUB_SCHEMA

ID: AMCLI-2351

Level: INFO

Description: Sub schema is added.

Data: name of service, schema type, name of sub schema

Triggers: Execute add sub schema Commandline interface.

FAILED_ADD_SUB_SCHEMA

ID: AMCLI-2352

Level: INFO

Description: Unable to add sub schema.

Data: name of service, schema type, name of sub schema, error message

Triggers: Execute add sub schema configurations Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_REMOVE_SUB_SCHEMA

ID: AMCLI-2360

Level: INFO

Description: Attempt to remove sub schema.

Data: name of service, schema type, name of parent sub schema, name of sub schema

Triggers: Execute remove sub schema Commandline interface.

SUCCEED_REMOVE_SUB_SCHEMA

ID: AMCLI-2361

Level: INFO

Description: Sub schema is removed.

Data: name of service, schema type, name of parent sub schema, name of sub schema

Triggers: Execute remove sub schema Commandline interface.

FAILED_REMOVE_SUB_SCHEMA

ID: AMCLI-2362

Level: INFO

Description: Unable to remove sub schema.

Data: name of service, schema type, name of parent sub schema, name of sub schema, error message

Triggers: Execute remove sub schema configurations Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_MODIFY_INHERITANCE_SUB_SCHEMA

ID: AMCLI-2370

Level: INFO

Description: Attempt to modify inheritance of sub schema.

Data: name of service, schema type, name of sub schema

Triggers: Execute modify inheritance of sub schema Commandline interface.

SUCCEED_MODIFY_INHERITANCE_SUB_SCHEMA

ID: AMCLI-2371

Level: INFO

Description: Sub schema is modified.

Data: name of service, schema type, name of sub schema

Triggers: Execute modify inheritance of sub schema Commandline interface.

FAILED_MODIFY_INHERITANCE_SUB_SCHEMA

ID: AMCLI-2372

Level: INFO

Description: Unable to modify sub schema.

Data: name of service, schema type, name of sub schema, error message

Triggers: Execute modify inheritance of sub schema configurations Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_MODIFY_SUB_CONFIGURATION

ID: AMCLI-2380

Level: INFO

Description: Attempt to modify sub configuration.

Data: name of sub configuration, name of service

Triggers: Execute modify sub configuration Commandline interface.

SUCCEED_MODIFY_SUB_CONFIGURATION

ID: AMCLI-2381

Level: INFO

Description: Sub configuration is modified.

Data: name of sub configuration, name of service

Triggers: Execute modify sub configuration Commandline interface.

FAILED_MODIFY_SUB_CONFIGURATION

ID: AMCLI-2382

Level: INFO

Description: Unable to modify sub configuration.

Data: name of sub configuration, name of service, error message

Triggers: Execute modify sub configuration Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_GET_SUB_CONFIGURATION

ID: AMCLI-2383

Level: INFO

Description: Attempt to retrieve sub configuration.

Data: name of sub configuration, name of service

Triggers: Execute get sub configuration Commandline interface.

SUCCEED_GET_SUB_CONFIGURATION

ID: AMCLI-2384

Level: INFO

Description: Sub configuration is retrieved.

Data: name of sub configuration, name of service

Triggers: Execute get sub configuration Commandline interface.

FAILED_GET_SUB_CONFIGURATION

ID: AMCLI-2385

Level: INFO

Description: Unable to retrieve sub configuration.

Data: name of sub configuration, name of service, error message

Triggers: Execute get sub configuration Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_MODIFY_SUB_CONFIGURATION_IN_REALM

ID: AMCLI-2390

Level: INFO

Description: Attempt to modify sub configuration in realm.

Data: name of realm, name of sub configuration, name of service

Triggers: Execute modify sub configuration Commandline interface.

SUCCEED_MODIFY_SUB_CONFIGURATION_IN_REALM

ID: AMCLI-2391

Level: INFO

Description: Sub configuration is modified.

Data: name of realm, name of sub configuration, name of service

Triggers: Execute modify sub configuration Commandline interface.

FAILED_MODIFY_SUB_CONFIGURATION_IN_REALM

ID: AMCLI-2392

Level: INFO

Description: Unable to modify sub configuration in realm.

Data: name of realm, name of sub configuration, name of service, error message

Triggers: Execute modify sub configuration Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_GET_SUB_CONFIGURATION_IN_REALM

ID: AMCLI-2393

Level: INFO

Description: Attempt to retrieve sub configuration in realm.

Data: name of realm, name of sub configuration, name of service

Triggers: Execute get sub configuration Commandline interface.

SUCCEED_GET_SUB_CONFIGURATION_IN_REALM

ID: AMCLI-2394

Level: INFO

Description: Sub configuration is retrieved.

Data: name of realm, name of sub configuration, name of service

Triggers: Execute get sub configuration Commandline interface.

FAILED_GET_SUB_CONFIGURATION_IN_REALM

ID: AMCLI-2395

Level: INFO

Description: Unable to retrieve sub configuration in realm.

Data: name of realm, name of sub configuration, name of service, error message

Triggers: Execute get sub configuration Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_ADD_PLUGIN_INTERFACE

ID: AMCLI-2400

Level: INFO

Description: Attempt to add Plug-in interface to service.

Data: name of service, name of plugin

Triggers: Execute add Plug-in interface Commandline interface.

SUCCEED_ADD_PLUGIN_INTERFACE

ID: AMCLI-2401

Level: INFO

Description: Plug-in interface is added.

Data: name of service, name of plugin

Triggers: Execute add Plug-in interface Commandline interface.

FAILED_ADD_PLUGIN_INTERFACE

ID: AMCLI-2402

Level: INFO

Description: Unable to add Plug-in interface to service.

Data: name of service, name of plugin, error message

Triggers: Execute add Plug-in interface Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_SET_PLUGIN_SCHEMA_PROP_VIEWBEAN_URL

ID: AMCLI-2410

Level: INFO

Description: Attempt to set Plug-in schema's properties view bean.

Data: name of service, name of plugin

Triggers: Execute set Plug-in schema's properties view bean Commandline interface.

SUCCEED_SET_PLUGIN_SCHEMA_PROP_VIEWBEAN_URL

ID: AMCLI-2411

Level: INFO

Description: Plug-in schema's properties view bean is set.

Data: name of service, name of plugin

Triggers: Execute set Plug-in schema's properties view bean Commandline interface.

FAILED_SET_PLUGIN_SCHEMA_PROP_VIEWBEAN_URL

ID: AMCLI-2412

Level: INFO

Description: Unable to set Plug-in schema's properties view bean.

Data: name of service, name of plugin, error message

Triggers: Execute set Plug-in schema's properties view bean Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_CREATE_POLICY_IN_REALM

ID: AMCLI-2420

Level: INFO

Description: Attempt to create policies under realm.

Data: name of realm

Triggers: Execute create policies under realm Commandline interface.

SUCCEED_CREATE_POLICY_IN_REALM

ID: AMCLI-2421

Level: INFO

Description: Policies are created.

Data: name of realm

Triggers: Execute create policies under realm Commandline interface.

FAILED_CREATE_POLICY_IN_REALM

ID: AMCLI-2422

Level: INFO

Description: Unable to create policies under realm.

Data: name of realm, error message

Triggers: Execute create policies under realm Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_DELETE_POLICY_IN_REALM

ID: AMCLI-2430

Level: INFO

Description: Attempt to delete policy in realm.

Data: name of realm, name of policy

Triggers: Execute delete policy in realm Commandline interface.

SUCCEED_DELETE_POLICY_IN_REALM

ID: AMCLI-2431

Level: INFO

Description: Policy is deleted.

Data: name of realm, name of policy

Triggers: Execute delete policy in realm Commandline interface.

FAILED_DELETE_POLICY_IN_REALM

ID: AMCLI-2432

Level: INFO

Description: Unable to delete policy under realm.

Data: name of realm, name of policy, error message

Triggers: Execute delete policy under realm Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_TO_GET_POLICY_NAMES_IN_REALM

ID: AMCLI-2433

Level: INFO

Description: Attempt to get policy names in realm.

Data: name of realm

Triggers: Execute get policy names in realm Commandline interface.

GOT_POLICY_NAMES_IN_REALM

ID: AMCLI-2434

Level: INFO

Description: Got policy names in realm.

Data: name of realm

Triggers: Execute get policy names in realm Commandline interface.

FAILED_GET_POLICY_NAMES_IN_REALM

ID: AMCLI-2435

Level: INFO

Description: Unable to get policy names in realm.

Data: name of realm

Triggers: Execute get policy names in realm Commandline interface.

ATTEMPT_GET_POLICY_IN_REALM

ID: AMCLI-2440

Level: INFO

Description: Attempt to get policy definition in realm.

Data: name of realm, name of policy

Triggers: Execute get policy definition in realm Commandline interface.

SUCCEED_GET_POLICY_IN_REALM

ID: AMCLI-2441

Level: INFO

Description: Policy definition is returned.

Data: name of realm, name of policy

Triggers: Execute get policy definition in realm Commandline interface.

FAILED_GET_POLICY_IN_REALM

ID: AMCLI-2442

Level: INFO

Description: Unable to get policy definition under realm.

Data: name of realm, name of policy, error message

Triggers: Execute get policy definition under realm Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_CREATE_IDENTITY

ID: AMCLI-2450

Level: INFO

Description: Attempt to create an identity in realm.

Data: name of realm, identity type, name of identity

Triggers: Execute create identity in realm Commandline interface.

SUCCEED_CREATE_IDENTITY

ID: AMCLI-2451

Level: INFO

Description: Identity is created.

Data: name of realm, identity type, name of identity

Triggers: Execute create identity in realm Commandline interface.

FAILED_CREATE_IDENTITY

ID: AMCLI-2452

Level: INFO

Description: Unable to create identity in realm.

Data: name of realm, identity type, name of identity, error message

Triggers: Execute create identity in realm Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_DELETE_IDENTITY

ID: AMCLI-2460

Level: INFO

Description: Attempt to delete an identity in realm.

Data: name of realm, identity type, name of identity

Triggers: Execute delete identity in realm Commandline interface.

SUCCEED_DELETE_IDENTITY

ID: AMCLI-2461

Level: INFO

Description: Identity is deleted.

Data: name of realm, identity type, name of identity

Triggers: Execute delete identity in realm Commandline interface.

FAILED_DELETE_IDENTITY

ID: AMCLI-2462

Level: INFO

Description: Unable to delete identity in realm.

Data: name of realm, identity type, name of identity, error message

Triggers: Execute delete identity in realm Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_SEARCH_IDENTITIES

ID: AMCLI-2470

Level: INFO

Description: Attempt to search identities in realm.

Data: name of realm, identity type, search pattern

Triggers: Execute search identities in realm Commandline interface.

SUCCEED_SEARCH_IDENTITIES

ID: AMCLI-2471

Level: INFO

Description: Search Result is returned.

Data: name of realm, identity type, search pattern

Triggers: Execute search identities in realm Commandline interface.

FAILED_SEARCH_IDENTITIES

ID: AMCLI-2472

Level: INFO

Description: Unable to search identities in realm.

Data: name of realm, identity type, search pattern, error message

Triggers: Execute search identities in realm Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_GET_ALLOWED_OPS

ID: AMCLI-2480

Level: INFO

Description: Attempt to get the allowed operation of an identity type in realm.

Data: name of realm, identity type

Triggers: Execute get the allowed operation of an identity type in realm Commandline interface.

SUCCEED_GET_ALLOWED_OPS

ID: AMCLI-2481

Level: INFO

Description: Allowed operations are returned.

Data: name of realm, identity type

Triggers: Execute get the allowed operation of an identity type in realm Commandline interface.

FAILED_GET_ALLOWED_OPS

ID: AMCLI-2482

Level: INFO

Description: Unable to get the allowed operation of an identity type in realm.

Data: name of realm, identity type, error message

Triggers: Execute get the allowed operation of an identity type in realm Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_GET_SUPPORTED_IDTYPES

ID: AMCLI-2490

Level: INFO

Description: Attempt to get the supported identity type in realm.

Data: name of realm

Triggers: Execute get the supported identity type in realm Commandline interface.

SUCCEED_GET_SUPPORTED_IDTYPES

ID: AMCLI-2491

Level: INFO

Description: Allowed identity types are returned.

Data: name of realm

Triggers: Execute get the supported identity type in realm Commandline interface.

FAILED_GET_SUPPORTED_IDTYPES

ID: AMCLI-2492

Level: INFO

Description: Unable to get the supported identity type in realm.

Data: name of realm, error message

Triggers: Execute get the supported identity type in realm Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_GET_ASSIGNABLE_SERVICES

ID: AMCLI-2500

Level: INFO

Description: Attempt to get the assignable services of an identity.

Data: name of realm, name of identity type, name of identity

Triggers: Execute get the assignable services of an identity Commandline interface.

SUCCEED_GET_ASSIGNABLE_SERVICES

ID: AMCLI-2501

Level: INFO

Description: Assignable services are returned.

Data: name of realm, name of identity type, name of identity

Triggers: Execute get the assignable services of an identity Commandline interface.

FAILED_GET_ASSIGNABLE_SERVICES

ID: AMCLI-2502

Level: INFO

Description: Unable to get the assignable services of an identity.

Data: name of realm, name of identity type, name of identity, error message

Triggers: Execute get the assignable services of an identity Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_GET_ASSIGNED_SERVICES

ID: AMCLI-2510

Level: INFO

Description: Attempt to get the assigned services of an identity.

Data: name of realm, name of identity type, name of identity

Triggers: Execute get the assigned services of an identity Commandline interface.

SUCCEED_GET_ASSIGNED_SERVICES

ID: AMCLI-2511

Level: INFO

Description: Assigned services are returned.

Data: name of realm, name of identity type, name of identity

Triggers: Execute get the assigned services of an identity Commandline interface.

FAILED_GET_ASSIGNED_SERVICES

ID: AMCLI-2512

Level: INFO

Description: Unable to get the assigned services of an identity.

Data: name of realm, name of identity type, name of identity, error message

Triggers: Execute get the assigned services of an identity Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_IDREPO_GET_SERVICE_ATTRIBUTES

ID: AMCLI-2520

Level: INFO

Description: Attempt to get service attribute values of an identity.

Data: name of realm, name of identity type, name of identity, name of service

Triggers: Execute get the service attribute values of an identity Commandline interface.

SUCCEED_IDREPO_GET_SERVICE_ATTRIBUTES

ID: AMCLI-2521

Level: INFO

Description: Service attribute values are returned.

Data: name of realm, name of identity type, name of identity, name of service

Triggers: Execute get the service attribute values of an identity Commandline interface.

FAILED_IDREPO_GET_SERVICE_ATTRIBUTES

ID: AMCLI-2522

Level: INFO

Description: Unable to get the service attribute values of an identity.

Data: name of realm, name of identity type, name of identity, name of service, error message

Triggers: Execute get the service attribute values of an identity Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_IDREPO_GET_ATTRIBUTES

ID: AMCLI-2530

Level: INFO

Description: Attempt to get attribute values of an identity.

Data: name of realm, name of identity type, name of identity

Triggers: Execute get the attribute values of an identity Commandline interface.

SUCCEED_IDREPO_GET_ATTRIBUTES

ID: AMCLI-2531

Level: INFO

Description: Attribute values are returned.

Data: name of realm, name of identity type, name of identity

Triggers: Execute get the attribute values of an identity Commandline interface.

FAILED_IDREPO_GET_ATTRIBUTES

ID: AMCLI-2532

Level: INFO

Description: Unable to get the attribute values of an identity.

Data: name of realm, name of identity type, name of identity, error message

Triggers: Execute get the attribute values of an identity Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_IDREPO_GET_MEMBERSHIPS

ID: AMCLI-2540

Level: INFO

Description: Attempt to get memberships of an identity.

Data: name of realm, name of identity type, name of identity, name of membership identity type

Triggers: Execute get the memberships of an identity Commandline interface.

SUCCEED_IDREPO_GET_MEMBERSHIPS

ID: AMCLI-2541

Level: INFO

Description: Memberships are returned.

Data: name of realm, name of identity type, name of identity, name of membership identity type

Triggers: Execute get the memberships of an identity Commandline interface.

FAILED_IDREPO_GET_MEMBERSHIPS

ID: AMCLI-2542

Level: INFO

Description: Unable to get the memberships of an identity.

Data: name of realm, name of identity type, name of identity, name of membership identity type, error message

Triggers: Execute get the memberships of an identity Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_IDREPO_GET_MEMBERS

ID: AMCLI-2550

Level: INFO

Description: Attempt to get members of an identity.

Data: name of realm, name of identity type, name of identity, name of membership identity type

Triggers: Execute get the members of an identity Commandline interface.

SUCCEED_IDREPO_GET_MEMBERS

ID: AMCLI-2551

Level: INFO

Description: Members are returned.

Data: name of realm, name of identity type, name of identity, name of membership identity type

Triggers: Execute get the members of an identity Commandline interface.

FAILED_IDREPO_GET_MEMBERS

ID: AMCLI-2552

Level: INFO

Description: Unable to get the members of an identity.

Data: name of realm, name of identity type, name of identity, name of membership identity type, error message

Triggers: Execute get the members of an identity Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_IDREPO_IS_MEMBER

ID: AMCLI-2560

Level: INFO

Description: Attempt to determine if an identity is a member of another identity.

Data: name of realm, name of identity type, name of identity, name of member identity type, name of member identity

Triggers: Execute determine if an identity is a member of another identity Commandline interface.

SUCCEED_IDREPO_IS_MEMBER

ID: AMCLI-2561

Level: INFO

Description: Membership is determined.

Data: name of realm, name of identity type, name of identity, name of member identity type, name of member identity

Triggers: Execute determine if an identity is a member of another identity Commandline interface.

FAILED_IDREPO_IS_MEMBER

ID: AMCLI-2562

Level: INFO

Description: Unable to determine the membership of an identity of another.

Data: name of realm, name of identity type, name of identity, name of member identity type, name of member identity, error message

Triggers: Execute determine if an identity is a member of another identity Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_IDREPO_IS_ACTIVE

ID: AMCLI-2570

Level: INFO

Description: Attempt to determine if an identity is active.

Data: name of realm, name of identity type, name of identity

Triggers: Execute determine if an identity is active Commandline interface.

SUCCEED_IDREPO_IS_ACTIVE

ID: AMCLI-2571

Level: INFO

Description: Active status of identity is determined.

Data: name of realm, name of identity type, name of identity

Triggers: Execute determine if an identity is active Commandline interface.

FAILED_IDREPO_IS_ACTIVE

ID: AMCLI-2572

Level: INFO

Description: Unable to determine if an identity is active.

Data: name of realm, name of identity type, name of identity, error message

Triggers: Execute determine if an identity is a active Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_IDREPO_ADD_MEMBER

ID: AMCLI-2580

Level: INFO

Description: Attempt to make an identity a member of another identity.

Data: name of realm, name of identity type, name of identity, name of member identity type, name of member identity

Triggers: Execute make an identity a member of another identity Commandline interface.

SUCCEED_IDREPO_ADD_MEMBER

ID: AMCLI-2581

Level: INFO

Description: Membership is set.

Data: name of realm, name of identity type, name of identity, name of member identity type, name of member identity

Triggers: Execute make an identity a member of another identity Commandline interface.

FAILED_IDREPO_ADD_MEMBER

ID: AMCLI-2582

Level: INFO

Description: Unable to add member of an identity to another.

Data: name of realm, name of identity type, name of identity, name of member identity type, name of member identity, error message

Triggers: Execute make an identity a member of another identity Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_IDREPO_REMOVE_MEMBER

ID: AMCLI-2590

Level: INFO

Description: Attempt to remove membership an identity from another identity.

Data: name of realm, name of identity type, name of identity, name of member identity type, name of member identity

Triggers: Execute remove membership an identity from another identity Commandline interface.

SUCCEED_IDREPO_REMOVE_MEMBER

ID: AMCLI-2591

Level: INFO

Description: Membership is removed.

Data: name of realm, name of identity type, name of identity, name of member identity type, name of member identity

Triggers: Execute remove membership an identity from another identity Commandline interface.

FAILED_IDREPO_REMOVE_MEMBER

ID: AMCLI-2592

Level: INFO

Description: Unable to remove membership of an identity.

Data: name of realm, name of identity type, name of identity, name of member identity type, name of member identity, error message

Triggers: Execute remove membership an identity from another identity Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_IDREPO_ASSIGN_SERVICE

ID: AMCLI-2600

Level: INFO

Description: Attempt to assign service to an identity.

Data: name of realm, identity type, name of identity, name of service

Triggers: Execute assign service to an identity Commandline interface.

SUCCEED_IDREPO_ASSIGN_SERVICE

ID: AMCLI-2601

Level: INFO

Description: Service is assigned to an identity.

Data: name of realm, identity type, name of identity, name of service

Triggers: Execute assign service to an identity Commandline interface.

FAILED_IDREPO_ASSIGN_SERVICE

ID: AMCLI-2602

Level: INFO

Description: Unable to assign service to an identity.

Data: name of realm, identity type, name of identity, name of service, error message

Triggers: Execute assign service to an identity Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_IDREPO_UNASSIGN_SERVICE

ID: AMCLI-2610

Level: INFO

Description: Attempt to unassign service from an identity.

Data: name of realm, identity type, name of identity, name of service

Triggers: Execute unassign service from an identity Commandline interface.

SUCCEED_IDREPO_UNASSIGN_SERVICE

ID: AMCLI-2611

Level: INFO

Description: Service is unassigned from an identity.

Data: name of realm, identity type, name of identity, name of service

Triggers: Execute unassign service from an identity Commandline interface.

FAILED_IDREPO_UNASSIGN_SERVICE

ID: AMCLI-2612

Level: INFO

Description: Unable to unassign service to an identity.

Data: name of realm, identity type, name of identity, name of service, error message

Triggers: Execute unassign service from an identity Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_IDREPO_MODIFY_SERVICE

ID: AMCLI-2620

Level: INFO

Description: Attempt to modify service attribute values of an identity.

Data: name of realm, identity type, name of identity, name of service

Triggers: Execute modify service attribute values of an identity Commandline interface.

SUCCEED_IDREPO_MODIFY_SERVICE

ID: AMCLI-2621

Level: INFO

Description: Service attribute values are modified.

Data: name of realm, identity type, name of identity, name of service

Triggers: Execute modify service attribute values of an identity Commandline interface.

FAILED_IDREPO_MODIFY_SERVICE

ID: AMCLI-2622

Level: INFO

Description: Unable to modify service attribute values of an identity.

Data: name of realm, identity type, name of identity, name of service, error message

Triggers: Execute modify service attribute values of an identity Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_IDREPO_SET_ATTRIBUTE_VALUES

ID: AMCLI-2630

Level: INFO

Description: Attempt to set attribute values of an identity.

Data: name of realm, identity type, name of identity

Triggers: Execute set attribute values of an identity Commandline interface.

SUCCEED_IDREPO_SET_ATTRIBUTE_VALUES

ID: AMCLI-2631

Level: INFO

Description: Attribute values are modified.

Data: name of realm, identity type, name of identity

Triggers: Execute set attribute values of an identity Commandline interface.

FAILED_IDREPO_SET_ATTRIBUTE_VALUES

ID: AMCLI-2632

Level: INFO

Description: Unable to set attribute values of an identity.

Data: name of realm, identity type, name of identity, error message

Triggers: Execute set attribute values of an identity Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_IDREPO_GET_PRIVILEGES

ID: AMCLI-2640

Level: INFO

Description: Attempt to get privileges of an identity.

Data: name of realm, identity type, name of identity

Triggers: Execute get privileges of an identity Commandline interface.

SUCCEED_IDREPO_GET_PRIVILEGES

ID: AMCLI-2641

Level: INFO

Description: Privileges are returned.

Data: name of realm, identity type, name of identity

Triggers: Execute get privileges of an identity Commandline interface.

FAILED_IDREPO_GET_PRIVILEGES

ID: AMCLI-2642

Level: INFO

Description: Unable to get privileges of an identity.

Data: name of realm, identity type, name of identity, error message

Triggers: Execute get privileges of an identity Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_IDREPO_ADD_PRIVILEGES

ID: AMCLI-2650

Level: INFO

Description: Attempt to add privileges to an identity.

Data: name of realm, identity type, name of identity

Triggers: Execute add privileges to an identity Commandline interface.

SUCCEED_IDREPO_ADD_PRIVILEGES

ID: AMCLI-2651

Level: INFO

Description: Privileges are added.

Data: name of realm, identity type, name of identity

Triggers: Execute add privileges to an identity Commandline interface.

FAILED_IDREPO_ADD_PRIVILEGES

ID: AMCLI-2652

Level: INFO

Description: Unable to add privileges to an identity.

Data: name of realm, identity type, name of identity, error message

Triggers: Execute add privileges to an identity Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_IDREPO_REMOVE_PRIVILEGES

ID: AMCLI-2660

Level: INFO

Description: Attempt to remove privileges from an identity.

Data: name of realm, identity type, name of identity

Triggers: Execute remove privileges from an identity Commandline interface.

SUCCEED_IDREPO_REMOVE_PRIVILEGES

ID: AMCLI-2661

Level: INFO

Description: Privileges are removed.

Data: name of realm, identity type, name of identity

Triggers: Execute remove privileges from an identity Commandline interface.

FAILED_IDREPO_REMOVE_PRIVILEGES

ID: AMCLI-2662

Level: INFO

Description: Unable to remove privileges from an identity.

Data: name of realm, identity type, name of identity, error message

Triggers: Execute remove privileges from an identity Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_SET_ATTRIBUTE_SCHEMA_BOOLEAN_VALUES

ID: AMCLI-2670

Level: INFO

Description: Attempt to set boolean values to attribute schema.

Data: name of service, schema type, name of sub schema, name of attribute schema

Triggers: Execute set attribute schema boolean values Commandline interface.

SUCCEED_SET_ATTRIBUTE_SCHEMA_BOOLEAN_VALUES

ID: AMCLI-2671

Level: INFO

Description: Boolean values are set.

Data: name of service, schema type, name of sub schema, name of attribute schema

Triggers: Execute set attribute schema boolean values Commandline interface.

FAILED_SET_ATTRIBUTE_SCHEMA_BOOLEAN_VALUES

ID: AMCLI-2672

Level: INFO

Description: Unable to set boolean values to attribute schema.

Data: name of service, schema type, name of sub schema, name of attribute schema, error message

Triggers: Execute set attribute schema boolean values Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_LIST_AUTH_INSTANCES

ID: AMCLI-2680

Level: INFO

Description: Attempt to list authentication instances.

Data: name of realm

Triggers: Execute list authentication instances Commandline interface.

SUCCEEDED_LIST_AUTH_INSTANCES

ID: AMCLI-2681

Level: INFO

Description: List authentication instances succeeded.

Data: name of realm

Triggers: Execute list authentication instances Commandline interface.

FAILED_LIST_AUTH_INSTANCES

ID: AMCLI-2682

Level: INFO

Description: Failed to list authentication instances.

Data: name of realm

Triggers: Execute list authentication instances Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_CREATE_AUTH_INSTANCE

ID: AMCLI-2690

Level: INFO

Description: Attempt to create authentication instance.

Data: name of realm, name of authentication instance, type of authentication instance

Triggers: Execute create authentication instance Commandline interface.

SUCCEEDED_CREATE_AUTH_INSTANCE

ID: AMCLI-2691

Level: INFO

Description: Authentication instance created.

Data: name of realm, name of authentication instance, type of authentication instance

Triggers: Execute create authentication instance Commandline interface.

FAILED_CREATE_AUTH_INSTANCE

ID: AMCLI-2692

Level: INFO

Description: Failed to create authentication instance.

Data: name of realm, name of authentication instance, type of authentication instance

Triggers: Execute create authentication instance Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_DELETE_AUTH_INSTANCES

ID: AMCLI-2700

Level: INFO

Description: Attempt to delete authentication instances.

Data: name of realm, name of authentication instances

Triggers: Execute delete authentication instance Commandline interface.

SUCCEEDED_DELETE_AUTH_INSTANCES

ID: AMCLI-2701

Level: INFO

Description: Authentication instances are deleted.

Data: name of realm, name of authentication instances

Triggers: Execute delete authentication instances Commandline interface.

FAILED_DELETE_AUTH_INSTANCES

ID: AMCLI-2702

Level: INFO

Description: Failed to delete authentication instance.

Data: name of realm, name of authentication instances

Triggers: Execute delete authentication instances Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_UPDATE_AUTH_INSTANCE

ID: AMCLI-2710

Level: INFO

Description: Attempt to update authentication instance.

Data: name of realm, name of authentication instance

Triggers: Execute update authentication instance Commandline interface.

SUCCEEDED_UPDATE_AUTH_INSTANCE

ID: AMCLI-2711

Level: INFO

Description: Authentication instance is updated.

Data: name of realm, name of authentication instance

Triggers: Execute update authentication instance Commandline interface.

FAILED_UPDATE_AUTH_INSTANCE

ID: AMCLI-2712

Level: INFO

Description: Failed to update authentication instance.

Data: name of realm, name of authentication instance

Triggers: Execute update authentication instance Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_GET_AUTH_INSTANCE

ID: AMCLI-2710

Level: INFO

Description: Attempt to get authentication instance.

Data: name of realm, name of authentication instance

Triggers: Execute get authentication instance Commandline interface.

SUCCEEDED_GET_AUTH_INSTANCE

ID: AMCLI-2711

Level: INFO

Description: Authentication instance profile is displayed.

Data: name of realm, name of authentication instance

Triggers: Execute get authentication instance Commandline interface.

FAILED_GET_AUTH_INSTANCE

ID: AMCLI-2712

Level: INFO

Description: Failed to get authentication instance.

Data: name of realm, name of authentication instance

Triggers: Execute get authentication instance Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_LIST_AUTH_CONFIGURATIONS

ID: AMCLI-2720

Level: INFO

Description: Attempt to list authentication configurations.

Data: name of realm

Triggers: Execute list authentication configurations Commandline interface.

SUCCEEDED_LIST_AUTH_CONFIGURATIONS

ID: AMCLI-2721

Level: INFO

Description: List authentication configurations succeeded.

Data: name of realm

Triggers: Execute list authentication configurations Commandline interface.

FAILED_LIST_AUTH_CONFIGURATIONS

ID: AMCLI-2722

Level: INFO

Description: Failed to list authentication configurations.

Data: name of realm

Triggers: Execute list authentication configurations Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_CREATE_AUTH_CONFIGURATION

ID: AMCLI-2730

Level: INFO

Description: Attempt to create authentication configuration.

Data: name of realm, name of authentication configuration

Triggers: Execute create authentication configuration Commandline interface.

SUCCEEDED_CREATE_AUTH_CONFIGURATION

ID: AMCLI-2731

Level: INFO

Description: Authentication configuration created.

Data: name of realm, name of authentication configuration

Triggers: Execute create authentication configuration Commandline interface.

FAILED_CREATE_AUTH_CONFIGURATION

ID: AMCLI-2732

Level: INFO

Description: Failed to create authentication configuration.

Data: name of realm, name of authentication configuration

Triggers: Execute create authentication configuration Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_DELETE_AUTH_CONFIGURATIONS

ID: AMCLI-2740

Level: INFO

Description: Attempt to delete authentication configurations.

Data: name of realm, name of authentication configurations

Triggers: Execute delete authentication configurations Commandline interface.

SUCCEEDED_DELETE_AUTH_CONFIGURATIONS

ID: AMCLI-2741

Level: INFO

Description: Authentication configurations are deleted.

Data: name of realm, name of authentication configurations

Triggers: Execute delete authentication configurations Commandline interface.

FAILED_DELETE_AUTH_CONFIGURATIONS

ID: AMCLI-2742

Level: INFO

Description: Failed to delete authentication instance.

Data: name of realm, name of authentication configurations

Triggers: Execute delete authentication configurations Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_GET_AUTH_CONFIG_ENTRIES

ID: AMCLI-2750

Level: INFO

Description: Attempt to get authentication configuration entries.

Data: name of realm, name of authentication configuration

Triggers: Execute get authentication configuration entries Commandline interface.

SUCCEEDED_GET_AUTH_CONFIG_ENTRIES

ID: AMCLI-2751

Level: INFO

Description: Authentication instance configuration entries are displayed.

Data: name of realm, name of authentication configuration

Triggers: Execute get authentication configuration entries Commandline interface.

FAILED_GET_AUTH_CONFIG_ENTRIES

ID: AMCLI-2752

Level: INFO

Description: Failed to get authentication configuration entries.

Data: name of realm, name of authentication configuration

Triggers: Execute get authentication configuration entries Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_SET_AUTH_CONFIG_ENTRIES

ID: AMCLI-2760

Level: INFO

Description: Attempt to set authentication configuration entries.

Data: name of realm, name of authentication configuration

Triggers: Execute set authentication configuration entries Commandline interface.

SUCCEEDED_SET_AUTH_CONFIG_ENTRIES

ID: AMCLI-2761

Level: INFO

Description: Authentication instance configuration entries are displayed.

Data: name of realm, name of authentication configuration

Triggers: Execute set authentication configuration entries Commandline interface.

FAILED_SET_AUTH_CONFIG_ENTRIES

ID: AMCLI-2762

Level: INFO

Description: Failed to set authentication configuration entries.

Data: name of realm, name of authentication configuration

Triggers: Execute set authentication configuration entries Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_LIST_DATASTORES

ID: AMCLI-2770

Level: INFO

Description: Attempt to list datastores.

Data: name of realm

Triggers: Execute list datastores Commandline interface.

SUCCEEDED_LIST_DATASTORES

ID: AMCLI-2771

Level: INFO

Description: List datastores succeeded.

Data: name of realm

Triggers: Execute list datastores Commandline interface.

FAILED_LIST_DATASTORES

ID: AMCLI-2772

Level: INFO

Description: Failed to list datastores.

Data: name of realm, error message

Triggers: Execute list datastores Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_CREATE_DATASTORE

ID: AMCLI-2780

Level: INFO

Description: Attemp to create datastore.

Data: name of realm, name of datastore, type of datastore

Triggers: Execute create datastore Commandline interface.

SUCCEEDED_CREATE_DATASTORE

ID: AMCLI-2781

Level: INFO

Description: Create datastore succeeded.

Data: name of realm, name of datastore, type of datastore

Triggers: Execute create datastore Commandline interface.

FAILED_CREATE_DATASTORE

ID: AMCLI-2782

Level: INFO

Description: Failed to create datastore.

Data: name of realm, name of datastore, type of datastore

Triggers: Execute create datastore Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_DELETE_DATASTORES

ID: AMCLI-2790

Level: INFO

Description: Attempt to delete datastores.

Data: name of realm, names of datastore

Triggers: Execute delete datastores Commandline interface.

SUCCEEDED_DELETE_DATASTORES

ID: AMCLI-2791

Level: INFO

Description: Delete datastores succeeded.

Data: name of realm, names of datastore

Triggers: Execute delete datastores Commandline interface.

FAILED_DELETE_DATASTORES

ID: AMCLI-2792

Level: INFO

Description: Failed to delete datastores.

Data: name of realm, names of datastore

Triggers: Execute delete datastore Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_UPDATE_DATASTORE

ID: AMCLI-2800

Level: INFO

Description: Attempt to update datastore profile.

Data: name of realm, name of datastore

Triggers: Execute update datastore Commandline interface.

SUCCEEDED_UPDATE_DATASTORE

ID: AMCLI-2801

Level: INFO

Description: Update datastore succeeded.

Data: name of realm, name of datastore

Triggers: Execute update datastore Commandline interface.

FAILED_UPDATE_DATASTORE

ID: AMCLI-2802

Level: INFO

Description: Failed to update datastore.

Data: name of realm, name of datastore, error message

Triggers: Execute update datastore Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_IMPORT_SM_CONFIG_DATA

ID: AMCLI-2900

Level: INFO

Description: Attempt to import service management configuration data.

Data: name of file

Triggers: Execute export configuration data Commandline interface.

SUCCEEDED_IMPORT_SM_CONFIG_DATA

ID: AMCLI-2901

Level: INFO

Description: Import service management configuration data succeeded.

Data: name of file

Triggers: Execute export configuration data Commandline interface.

FAILED_IMPORT_SM_CONFIG_DATA

ID: AMCLI-2902

Level: INFO

Description: Failed to import service management configuration data.

Data: name of file, error message

Triggers: Execute export configuration data Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_EXPORT_SM_CONFIG_DATA

ID: AMCLI-3000

Level: INFO

Description: Attempt to export service management configuration data.

Data: name of file

Triggers: Execute export configuration data Commandline interface.

SUCCEEDED_IMPORT_SM_CONFIG_DATA

ID: AMCLI-3001

Level: INFO

Description: Export service management configuration data succeeded.

Data: name of file

Triggers: Execute export configuration data Commandline interface.

FAILED_EXPORT_SM_CONFIG_DATA

ID: AMCLI-3002

Level: INFO

Description: Failed to export service management configuration data.

Data: name of file, error message

Triggers: Execute export configuration data Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_CREATE_SERVERCONFIG_XML

ID: AMCLI-3010

Level: INFO

Description: Attempt to create server configuration xml.

Data: name of file

Triggers: Execute create server configuration xml Commandline interface.

SUCCEEDED_CREATE_SERVERCONFIG_XML

ID: AMCLI-3011

Level: INFO

Description: Create server configuration xml succeeded.

Data: name of file

Triggers: Execute create server configuration xml Commandline interface.

FAILED_CREATE_SERVERCONFIG_XML

ID: AMCLI-3012

Level: INFO

Description: Failed to create server configuration xml.

Data: name of file, error message

Triggers: Execute create server configuration xml Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_REALM_REMOVE_SERVICE_ATTR_VALUES

ID: AMCLI-3020

Level: INFO

Description: Attempt to remove service attribute values of realm.

Data: name of realm, name of service

Triggers: Execute remove service attribute values of realm Commandline interface.

SUCCEED_REALM_REMOVE_SERVICE_ATTR_VALUES

ID: AMCLI-3021

Level: INFO

Description: Service attribute values of realm are removed.

Data: name of realm, name of service

Triggers: Execute remove service attribute values of realm Commandline interface.

FAILED_REALM_REMOVE_SERVICE_ATTR_VALUES

ID: AMCLI-3022

Level: INFO

Description: Unable to remove service attribute values of realm.

Data: name of realm, name of service, error message

Triggers: Execute remove service attribute values of realm Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_REALM_ADD_SERVICE_ATTR_VALUES

ID: AMCLI-3030

Level: INFO

Description: Attempt to add service attribute values of realm.

Data: name of realm, name of service

Triggers: Execute add service attribute values of realm Commandline interface.

SUCCEED_REALM_ADD_SERVICE_ATTR_VALUES

ID: AMCLI-3031

Level: INFO

Description: Service attribute values of realm are added.

Data: name of realm, name of service

Triggers: Execute add service attribute values of realm Commandline interface.

FAILED_REALM_ADD_SERVICE_ATTR_VALUES

ID: AMCLI-3032

Level: INFO

Description: Unable to add service attribute values of realm.

Data: name of realm, name of service, error message

Triggers: Execute add service attribute values of realm Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_LIST_SERVER_CONFIG

ID: AMCLI-3040

Level: INFO

Description: Attempt to list server configuration.

Data: name of server

Triggers: Execute list server configuration Commandline interface.

SUCCEED_LIST_SERVER_CONFIG

ID: AMCLI-3041

Level: INFO

Description: Server configuration is displayed.

Data: name of server

Triggers: Execute list server configuration Commandline interface.

FAILED_LIST_SERVER_CONFIG

ID: AMCLI-3042

Level: INFO

Description: Unable to list server configuration.

Data: name of server, error message

Triggers: Execute list server configuration Commandline interface.

Actions: Check if servername is correct.; Look under debug file for more information.

ATTEMPT_UPDATE_SERVER_CONFIG

ID: AMCLI-3050

Level: INFO

Description: Attempt to update server configuration.

Data: name of server

Triggers: Execute update server configuration Commandline interface.

SUCCEED_UPDATE_SERVER_CONFIG

ID: AMCLI-3051

Level: INFO

Description: Server configuration is updated.

Data: name of server

Triggers: Execute update server configuration Commandline interface.

FAILED_UPDATE_SERVER_CONFIG

ID: AMCLI-3052

Level: INFO

Description: Unable to update server configuration.

Data: name of server, error message

Triggers: Execute update server configuration Commandline interface.

Actions: Check if servername is correct.; Look under debug file for more information.

ATTEMPT_REMOVE_SERVER_CONFIG

ID: AMCLI-3060

Level: INFO

Description: Attempt to remove server configuration.

Data: name of server

Triggers: Execute remove server configuration Commandline interface.

SUCCEED_REMOVE_SERVER_CONFIG

ID: AMCLI-3061

Level: INFO

Description: Server configuration is removed.

Data: name of server

Triggers: Execute remove server configuration Commandline interface.

FAILED_REMOVE_SERVER_CONFIG

ID: AMCLI-3062

Level: INFO

Description: Remove server configuration.

Data: name of server, error message

Triggers: Execute remove server configuration Commandline interface.

Actions: Check if servername is correct.; Look under debug file for more information.

ATTEMPT_CREATE_SERVER

ID: AMCLI-3070

Level: INFO

Description: Attempt to create server.

Data: name of server

Triggers: Execute create server Commandline interface.

SUCCEED_CREATE_SERVER

ID: AMCLI-3071

Level: INFO

Description: Server is created.

Data: name of server

Triggers: Execute create server Commandline interface.

FAILED_CREATE_SERVER

ID: AMCLI-3072

Level: INFO

Description: Unable to create server.

Data: name of server, error message

Triggers: Execute create server Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_DELETE_SERVER

ID: AMCLI-3080

Level: INFO

Description: Attempt to delete server.

Data: name of server

Triggers: Execute delete server Commandline interface.

SUCCEED_DELETE_SERVER

ID: AMCLI-3081

Level: INFO

Description: Server is deleted.

Data: name of server

Triggers: Execute delete server Commandline interface.

FAILED_DELETE_SERVER

ID: AMCLI-3082

Level: INFO

Description: Unable to delete server.

Data: name of server, error message

Triggers: Execute delete server Commandline interface.

Actions: Check the name of the server.; Look under debug file for more information.

ATTEMPT_LIST_SERVERS

ID: AMCLI-3090

Level: INFO

Description: Attempt to list servers.

Triggers: Execute list servers Commandline interface.

SUCCEED_LIST_SERVERS

ID: AMCLI-3091

Level: INFO

Description: Servers are displayed.

Triggers: Execute list servers Commandline interface.

FAILED_LIST_SERVERS

ID: AMCLI-3092

Level: INFO

Description: Unable to list servers.

Data: error message

Triggers: Execute list servers Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_CREATE_SITE

ID: AMCLI-3100

Level: INFO

Description: Attempt to create site.

Data: name of site, primary URL of site

Triggers: Execute create site Commandline interface.

SUCCEED_CREATE_SITE

ID: AMCLI-3101

Level: INFO

Description: Site is created.

Data: name of site, primary URL of site

Triggers: Execute create site Commandline interface.

FAILED_CREATE_SITE

ID: AMCLI-3102

Level: INFO

Description: Unable to create site.

Data: name of site, primary URL of site, error message

Triggers: Execute create site Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_LIST_SITES

ID: AMCLI-3110

Level: INFO

Description: Attempt to list sites.

Triggers: Execute list sites Commandline interface.

SUCCEED_LIST_SITES

ID: AMCLI-3111

Level: INFO

Description: Sites are displayed.

Triggers: Execute list sites Commandline interface.

FAILED_LIST_SITES

ID: AMCLI-3112

Level: INFO

Description: Unable to list sites.

Data: error message

Triggers: Execute list sites Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_SHOW_SITE_MEMBERS

ID: AMCLI-3120

Level: INFO

Description: Attempt to show site members.

Data: name of site

Triggers: Execute show site members Commandline interface.

SUCCEED_SHOW_SITE_MEMBERS

ID: AMCLI-3121

Level: INFO

Description: Site members are displayed.

Data: name of site

Triggers: Execute show site members Commandline interface.

FAILED_SHOW_SITE_MEMBERS

ID: AMCLI-3122

Level: INFO

Description: Unable to show site members.

Data: name of site, error message

Triggers: Execute show site members Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_ADD_SITE_MEMBERS

ID: AMCLI-3130

Level: INFO

Description: Attempt to add members to site.

Data: name of site

Triggers: Execute add members to site Commandline interface.

SUCCEED_ADD_SITE_MEMBERS

ID: AMCLI-3131

Level: INFO

Description: Members are added to site.

Data: name of site

Triggers: Execute add members to site Commandline interface.

FAILED_ADD_SITE_MEMBERS

ID: AMCLI-3132

Level: INFO

Description: Unable to add members to site.

Data: name of site, error message

Triggers: Execute add members to site Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_REMOVE_SITE_MEMBERS

ID: AMCLI-3140

Level: INFO

Description: Attempt to remove members from site.

Data: name of site

Triggers: Execute remove members from site Commandline interface.

SUCCEED_REMOVE_SITE_MEMBERS

ID: AMCLI-3141

Level: INFO

Description: Members are removed from site.

Data: name of site

Triggers: Execute remove members from site Commandline interface.

FAILED_REMOVE_SITE_MEMBERS

ID: AMCLI-3142

Level: INFO

Description: Unable to remove members from site.

Data: name of site, error message

Triggers: Execute remove members from site Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_DELETE_SITE

ID: AMCLI-3150

Level: INFO

Description: Attempt to delete site.

Data: name of site

Triggers: Execute delete site Commandline interface.

SUCCEED_DELETE_SITE

ID: AMCLI-3151

Level: INFO

Description: Site is deleted.

Data: name of site

Triggers: Execute delete site Commandline interface.

FAILED_DELETE_SITE

ID: AMCLI-3152

Level: INFO

Description: Unable to delete members from site.

Data: name of site, error message

Triggers: Execute delete site Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_SET_SITE_PRIMARY_URL

ID: AMCLI-3160

Level: INFO

Description: Attempt to set site primary URL.

Data: name of site, primary URL of site

Triggers: Execute set site primary URL Commandline interface.

SUCCEED_SET_SITE_PRIMARY_URL

ID: AMCLI-3161

Level: INFO

Description: Site primary URL is set.

Data: name of site, primary URL of site

Triggers: Execute set site primary URL Commandline interface.

FAILED_SET_SITE_PRIMARY_URL

ID: AMCLI-3162

Level: INFO

Description: Unable to set site primary URL.

Data: name of site, primary URL of site, error message

Triggers: Execute set site primary URL Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_SHOW_SITE

ID: AMCLI-3170

Level: INFO

Description: Attempt to show site profile.

Data: name of site

Triggers: Execute show site profile Commandline interface.

SUCCEED_SHOW_SITE

ID: AMCLI-3171

Level: INFO

Description: Site profile is displayed.

Data: name of site

Triggers: Execute show site profile Commandline interface.

FAILED_SHOW_SITE

ID: AMCLI-3172

Level: INFO

Description: Unable to show site profile.

Data: name of site, error message

Triggers: Execute show site profile Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_SET_SITE_FAILOVER_URLS

ID: AMCLI-3180

Level: INFO

Description: Attempt to set site failover URLs.

Data: name of site

Triggers: Execute set site failover URLs Commandline interface.

SUCCEED_SET_SITE_FAILOVER_URLS

ID: AMCLI-3181

Level: INFO

Description: Site failover URLs are set.

Data: name of site

Triggers: Execute set site failover URLs Commandline interface.

FAILED_SET_SITE_FAILOVER_URLS

ID: AMCLI-3182

Level: INFO

Description: Unable to set site failover URLs.

Data: name of site, error message

Triggers: Execute set site failover URLs Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_ADD_SITE_FAILOVER_URLS

ID: AMCLI-3190

Level: INFO

Description: Attempt to add site failover URLs.

Data: name of site

Triggers: Execute add site failover URLs Commandline interface.

SUCCEED_ADD_SITE_FAILOVER_URLS

ID: AMCLI-3191

Level: INFO

Description: Site failover URLs are added.

Data: name of site

Triggers: Execute add site failover URLs Commandline interface.

FAILED_ADD_SITE_FAILOVER_URLS

ID: AMCLI-3192

Level: INFO

Description: Unable to add site failover URLs.

Data: name of site, error message

Triggers: Execute add site failover URLs Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_REMOVE_SITE_FAILOVER_URLS

ID: AMCLI-3200

Level: INFO

Description: Attempt to remove site failover URLs.

Data: name of site

Triggers: Execute remove site failover URLs Commandline interface.

SUCCEED_REMOVE_SITE_FAILOVER_URLS

ID: AMCLI-3201

Level: INFO

Description: Site failover URLs are removed.

Data: name of site

Triggers: Execute remove site failover URLs Commandline interface.

FAILED_REMOVE_SITE_FAILOVER_URLS

ID: AMCLI-3202

Level: INFO

Description: Unable to remove site failover URLs.

Data: name of site, error message

Triggers: Execute remove site failover URLs Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_CLONE_SERVER

ID: AMCLI-3210

Level: INFO

Description: Attempt to clone server.

Data: name of server, name of cloned server

Triggers: Execute clone server Commandline interface.

SUCCEED_CLONE_SERVER

ID: AMCLI-3211

Level: INFO

Description: Server is cloned.

Data: name of server, name of cloned server

Triggers: Execute clone server Commandline interface.

FAILED_CLONE_SERVER

ID: AMCLI-3212

Level: INFO

Description: Unable to clone server.

Data: name of server, name of cloned server, error message

Triggers: Execute clone server Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_EXPORT_SERVER

ID: AMCLI-3220

Level: INFO

Description: Attempt to export server.

Data: name of server

Triggers: Execute export server Commandline interface.

SUCCEED_EXPORT_SERVER

ID: AMCLI-3221

Level: INFO

Description: Server is cloned.

Data: name of server

Triggers: Execute export server Commandline interface.

FAILED_EXPORT_SERVER

ID: AMCLI-3222

Level: INFO

Description: Unable to export server.

Data: name of server, error message

Triggers: Execute export server Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_IMPORT_SERVER

ID: AMCLI-3230

Level: INFO

Description: Attempt to import server configuration.

Data: name of server

Triggers: Execute import server configuration Commandline interface.

SUCCEED_IMPORT_SERVER

ID: AMCLI-3231

Level: INFO

Description: Server configuration is imported.

Data: name of server

Triggers: Execute import server configuration Commandline interface.

FAILED_IMPORT_SERVER

ID: AMCLI-3232

Level: INFO

Description: Unable to import server configuration.

Data: name of server, error message

Triggers: Execute import server configuration Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_GET_SUPPORTED_DATA_TYPES

ID: AMCLI-5000

Level: INFO

Description: Attempt to get the supported data types.

Triggers: Execute get the supported data type Commandline interface.

SUCCEED_GET_SUPPORTED_DATA_TYPES

ID: AMCLI-5001

Level: INFO

Description: The supported data types are retrieved.

Triggers: Execute add service attribute values Commandline interface.

FAILED_GET_SUPPORTED_DATA_TYPES

ID: AMCLI-5002

Level: INFO

Description: Unable to get the supported data types.

Data: error message

Triggers: Execute get the supported data types Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_CREATE_AGENT

ID: AMCLI-4000

Level: INFO

Description: Attempt to create an agent.

Data: realm, agent type, name of agent

Triggers: Execute create agent Commandline interface.

SUCCEED_CREATE_AGENT

ID: AMCLI-4001

Level: INFO

Description: Agent is created.

Data: realm, agent type, name of agent

Triggers: Execute create agent Commandline interface.

FAILED_CREATE_AGENT

ID: AMCLI-4002

Level: INFO

Description: Unable to create agent.

Data: realm, agent type, name of agent, error message

Triggers: Execute create agent Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_DELETE_AGENTS

ID: AMCLI-4010

Level: INFO

Description: Attempt to delete agents.

Data: name of realm, name of agents

Triggers: Execute delete agents Commandline interface.

SUCCEED_DELETE_AGENTS

ID: AMCLI-4011

Level: INFO

Description: Agents are deleted.

Data: name of realm, name of agents

Triggers: Execute delete agents Commandline interface.

FAILED_DELETE_AGENTS

ID: AMCLI-4012

Level: INFO

Description: Unable to delete agents.

Data: name of realm, name of agents, error message

Triggers: Execute delete agents Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_UPDATE_AGENT

ID: AMCLI-4020

Level: INFO

Description: Attempt to set attribute values of an agent.

Data: name of realm, name of agent

Triggers: Execute update agent Commandline interface.

SUCCEED_UPDATE_AGENT

ID: AMCLI-4021

Level: INFO

Description: Agent profile is modified.

Data: name of realm, name of agent

Triggers: Execute update agent Commandline interface.

FAILED_UPDATE_AGENT

ID: AMCLI-4022

Level: INFO

Description: Unable to update an agent.

Data: name of realm, name of agent, error message

Triggers: Execute update agent Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_LIST_AGENTS

ID: AMCLI-4030

Level: INFO

Description: Attempt to list agents.

Data: name of realm, agent type, search pattern

Triggers: Execute list agents Commandline interface.

SUCCEED_LIST_AGENTS

ID: AMCLI-4031

Level: INFO

Description: Search Result is returned.

Data: name of realm, agent type, search pattern

Triggers: Execute list agents Commandline interface.

FAILED_LIST_AGENTS

ID: AMCLI-4032

Level: INFO

Description: Unable to list agents.

Data: name of realm, agent type, search pattern, error message

Triggers: Execute list agents Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_SHOW_AGENT

ID: AMCLI-4040

Level: INFO

Description: Attempt to get attribute values of an agent.

Data: name of realm, name of agent

Triggers: Execute get the attribute values of an agent Commandline interface.

SUCCEED_SHOW_AGENT

ID: AMCLI-4041

Level: INFO

Description: Attribute values are returned.

Data: name of realm, name of agent

Triggers: Execute get the attribute values of an agent Commandline interface.

FAILED_SHOW_AGENT

ID: AMCLI-4042

Level: INFO

Description: Unable to get the attribute values of an agent.

Data: name of realm, name of agent, error message

Triggers: Execute get the attribute values of an agent Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_CREATE_AGENT_GROUP

ID: AMCLI-4050

Level: INFO

Description: Attempt to create an agent group.

Data: realm, agent type, name of agent group

Triggers: Execute create agent group Commandline interface.

SUCCEED_CREATE_AGENT_GROUP

ID: AMCLI-4051

Level: INFO

Description: Agent group is created.

Data: realm, agent type, name of agent group

Triggers: Execute create agent group Commandline interface.

FAILED_CREATE_AGENT_GROUP

ID: AMCLI-4052

Level: INFO

Description: Unable to create agent group.

Data: realm, agent type, name of agent group, error message

Triggers: Execute create agent group Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_DELETE_AGENT_GROUPS

ID: AMCLI-4060

Level: INFO

Description: Attempt to delete agent groups.

Data: name of realm, name of agent groups

Triggers: Execute delete agent groups Commandline interface.

SUCCEED_DELETE_AGENT_GROUPS

ID: AMCLI-4061

Level: INFO

Description: Agent groups are deleted.

Data: name of realm, name of agent groups

Triggers: Execute delete agent groups Commandline interface.

FAILED_DELETE_AGENT_GROUPS

ID: AMCLI-4062

Level: INFO

Description: Unable to delete agent groups.

Data: name of realm, name of agent groups, error message

Triggers: Execute delete agent groups Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_LIST_AGENT_GROUPS

ID: AMCLI-4070

Level: INFO

Description: Attempt to list agent groups.

Data: name of realm, agent type, search pattern

Triggers: Execute list agent groups Commandline interface.

SUCCEED_LIST_AGENT_GROUPS

ID: AMCLI-4071

Level: INFO

Description: Search Result is returned.

Data: name of realm, agent type, search pattern

Triggers: Execute list agent groups Commandline interface.

FAILED_LIST_AGENT_GROUPS

ID: AMCLI-4072

Level: INFO

Description: Unable to list agent groups.

Data: name of realm, agent type, search pattern, error message

Triggers: Execute list agent groups Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_ADD_AGENT_TO_GROUP

ID: AMCLI-4080

Level: INFO

Description: Attempt to add agent to group.

Data: name of realm, name of agent group, name of agent

Triggers: Execute add agents to group Commandline interface.

SUCCEED_ADD_AGENT_TO_GROUP

ID: AMCLI-4081

Level: INFO

Description: Agent is added to group.

Data: name of realm, name of agent group, name of agent

Triggers: Execute add agent to group Commandline interface.

FAILED_ADD_AGENT_TO_GROUP

ID: AMCLI-4082

Level: INFO

Description: Unable to add agent to group.

Data: name of realm, name of agent group, name of agent, error message

Triggers: Execute add agent to group Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_REMOVE_AGENT_FROM_GROUP

ID: AMCLI-4090

Level: INFO

Description: Attempt to remove agent from group.

Data: name of realm, name of agent group, name of agent

Triggers: Execute remove agent from group Commandline interface.

SUCCEED_REMOVE_AGENT_FROM_GROUP

ID: AMCLI-4091

Level: INFO

Description: Agent is removed to group.

Data: name of realm, name of agent group, name of agent

Triggers: Execute remove agent from group Commandline interface.

FAILED_REMOVE_AGENT_FROM_GROUP

ID: AMCLI-4092

Level: INFO

Description: Unable to remove agent from group.

Data: name of realm, name of agent group, name of agent, error message

Triggers: Execute remove agent from group Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_SET_AGENT_PWD

ID: AMCLI-4100

Level: INFO

Description: Attempt to set agent password.

Data: realm, name of agent

Triggers: Execute set agent password Commandline interface.

SUCCEED_SET_AGENT_PWD

ID: AMCLI-4101

Level: INFO

Description: Agent password is modified.

Data: realm, name of agent

Triggers: Execute set agent password Commandline interface.

FAILED_SET_AGENT_PWD

ID: AMCLI-4102

Level: INFO

Description: Unable to set agent password.

Data: realm, name of agent, error message

Triggers: Execute set agent password Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_SHOW_AGENT_GROUP

ID: AMCLI-4110

Level: INFO

Description: Attempt to get attribute values of an agent group.

Data: name of realm, name of agent group

Triggers: Execute get the attribute values of an agent group Commandline interface.

SUCCEED_SHOW_AGENT_GROUP

ID: AMCLI-4111

Level: INFO

Description: Attribute values are returned.

Data: name of realm, name of agent group

Triggers: Execute get the attribute values of an agent group Commandline interface.

FAILED_SHOW_AGENT_GROUP

ID: AMCLI-4112

Level: INFO

Description: Unable to get the attribute values of an agent group.

Data: name of realm, name of agent group, error message

Triggers: Execute get the attribute values of an agent group Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_UPDATE_AGENT_GROUP

ID: AMCLI-4120

Level: INFO

Description: Attempt to set attribute values of an agent group.

Data: name of realm, name of agent group

Triggers: Execute update agent group Commandline interface.

SUCCEED_UPDATE_AGENT_GROUP

ID: AMCLI-4121

Level: INFO

Description: Agent group profile is modified.

Data: name of realm, name of agent group

Triggers: Execute update agent group Commandline interface.

FAILED_UPDATE_AGENT_GROUP

ID: AMCLI-4122

Level: INFO

Description: Unable to update an agent.

Data: name of realm, name of agent group, error message

Triggers: Execute update agent group Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_SHOW_AGENT_TYPES

ID: AMCLI-4130

Level: INFO

Description: Attempt to show supported agent types.

Triggers: Execute show supported agent types Commandline interface.

SUCCEED_SHOW_AGENT_TYPES

ID: AMCLI-4131

Level: INFO

Description: Supported agent types is displayed.

Triggers: Execute show supported agent types Commandline interface.

FAILED_SHOW_AGENT_TYPES

ID: AMCLI-4132

Level: INFO

Description: Unable to show supported agent types.

Data: error message

Triggers: Execute show supported agent types Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_SHOW_AGENT_GROUP_MEMBERS

ID: AMCLI-4140

Level: INFO

Description: Attempt to show agent group members.

Data: name of realm, name of agent group

Triggers: Execute show agent group members Commandline interface.

SUCCEED_SHOW_AGENT_GROUP_MEMBERS

ID: AMCLI-4141

Level: INFO

Description: Agent group's members are displayed.

Data: name of realm, name of agent group

Triggers: Execute show agent group members Commandline interface.

FAILED_SHOW_AGENT_GROUP_MEMBERS

ID: AMCLI-4142

Level: INFO

Description: Unable to show agent group members.

Data: name of realm, name of agent group, error message

Triggers: Execute show agent group members Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_LIST_AGENT_MEMBERSHIP

ID: AMCLI-4150

Level: INFO

Description: Attempt to show agent's membership.

Data: name of realm, name of agent

Triggers: Execute show agent's membership Commandline interface.

SUCCEED_LIST_AGENT_MEMBERSHIP

ID: AMCLI-4151

Level: INFO

Description: Agent's membership are displayed.

Data: name of realm, name of agent

Triggers: Execute show agent's membership Commandline interface.

FAILED_LIST_AGENT_MEMBERSHIP

ID: AMCLI-4152

Level: INFO

Description: Unable to show agent's membership.

Data: name of realm, name of agent, error message

Triggers: Execute show agent's membership Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_REGISTER_AUTH_MODULE

ID: AMCLI-4500

Level: INFO

Description: Attempt to register authentication module.

Data: name of service

Triggers: Execute register authentication module Commandline interface.

SUCCEED_REGISTER_AUTH_MODULE

ID: AMCLI-4501

Level: INFO

Description: Authentication module is registered.

Data: name of service

Triggers: Execute register authentication module Commandline interface.

FAILED_REGISTER_AUTH_MODULE

ID: AMCLI-4502

Level: INFO

Description: Unable to register authentication module.

Data: name of service, error message

Triggers: Execute register authentication module Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_UNREGISTER_AUTH_MODULE

ID: AMCLI-4510

Level: INFO

Description: Attempt to unregister authentication module.

Data: name of service

Triggers: Execute unregister authentication module Commandline interface.

SUCCEED_UNREGISTER_AUTH_MODULE

ID: AMCLI-4511

Level: INFO

Description: Authentication module is unregistered.

Data: name of service

Triggers: Execute unregister authentication module Commandline interface.

FAILED_UNREGISTER_AUTH_MODULE

ID: AMCLI-4512

Level: INFO

Description: Unable to unregister authentication module.

Data: name of service, error message

Triggers: Execute unregister authentication module Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_GET_SUPPORTED_AUTH_MODULES

ID: AMCLI-4515

Level: INFO

Description: Attempt to get supported authentication modules in the system.

Triggers: Execute get supported authentication modules in the system Commandline interface.

SUCCEED_GET_SUPPORTED_AUTH_MODULES

ID: AMCLI-4516

Level: INFO

Description: Supported authentication modules in the system are displayed.

Triggers: Execute get supported authentication modules in the system module Commandline interface.

FAILED_GET_SUPPORTED_AUTH_MODULES

ID: AMCLI-4517

Level: INFO

Description: Failed to get supported authentication modules in the system.

Data: error message

Triggers: Execute get supported authentication modules in the system Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_REMOVE_AGENT_PROPERTIES

ID: AMCLI-4520

Level: INFO

Description: Attempt to remove property values of an agent.

Data: name of realm, name of agent, property names

Triggers: Execute remove property values of an agent Commandline interface.

SUCCEED_REMOVE_AGENT_PROPERTIES

ID: AMCLI-4521

Level: INFO

Description: Property values are removed.

Data: name of realm, name of agent, property names

Triggers: Execute remove property values of an agent Commandline interface.

FAILED_REMOVE_AGENT_PROPERTIES

ID: AMCLI-4522

Level: INFO

Description: Unable to remove property values of an agent.

Data: name of realm, name of agent, property names, error message

Triggers: Execute remove property values of an agent Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_GET_SERVER_CONFIG_XML

ID: AMCLI-4600

Level: INFO

Description: Attempt to get server configuration XML.

Data: name of server

Triggers: Execute get server configuration XML Commandline interface.

SUCCEED_GET_SERVER_CONFIG_XML

ID: AMCLI-4601

Level: INFO

Description: Server configuration XML is displayed.

Data: name of server

Triggers: Execute get server configuration XML Commandline interface.

FAILED_GET_SERVER_CONFIG_XML

ID: AMCLI-4602

Level: INFO

Description: Unable to get server configuration XML.

Data: name of server, error message

Triggers: Execute get server configuration XML Commandline interface.

Actions: Check if servername is correct.; Look under debug file for more information.

ATTEMPT_SET_SERVER_CONFIG_XML

ID: AMCLI-4610

Level: INFO

Description: Attempt to set server configuration XML.

Data: name of server

Triggers: Execute set server configuration XML Commandline interface.

SUCCEED_SET_SERVER_CONFIG_XML

ID: AMCLI-4611

Level: INFO

Description: Server configuration XML is set.

Data: name of server

Triggers: Execute set server configuration XML Commandline interface.

FAILED_SET_SERVER_CONFIG_XML

ID: AMCLI-4612

Level: INFO

Description: Unable to set server configuration XML.

Data: name of server, error message

Triggers: Execute set server configuration XML Commandline interface.

Actions: Check if servername is correct.; Look under debug file for more information.

ATTEMPT_LIST_DATASTORE_TYPES

ID: AMCLI-4700

Level: INFO

Description: Attempt to list supported datastore types.

Triggers: Execute list supported datastore types Commandline interface.

SUCCEEDED_LIST_DATASTORE_TYPES

ID: AMCLI-4701

Level: INFO

Description: List supported datastore types succeeded.

Triggers: Execute list supported datastore types Commandline interface.

FAILED_LIST_DATASTORE_TYPES

ID: AMCLI-4702

Level: INFO

Description: Failed to list supported datastore types.

Data: error message

Triggers: Execute list supported datastore types Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_ADD_AUTH_CONFIG_ENTRY

ID: AMCLI-4800

Level: INFO

Description: Attempt to add authentication configuration entry.

Data: name of realm, name of authentication configuration, name of module

Triggers: Execute add authentication configuration entry Commandline interface.

SUCCEEDED_ADD_AUTH_CONFIG_ENTRY

ID: AMCLI-4801

Level: INFO

Description: Authentication instance configuration entry is created.

Data: name of realm, name of authentication configuration, name of module

Triggers: Execute add authentication configuration entry Commandline interface.

FAILED_ADD_AUTH_CONFIG_ENTRY

ID: AMCLI-4802

Level: INFO

Description: Failed to add authentication configuration entry.

Data: name of realm, name of authentication configuration, name of module, error message

Triggers: Execute add authentication configuration entry Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_SHOW_DATASTORE

ID: AMCLI-5000

Level: INFO

Description: Attempt to show datastore profile.

Data: name of realm, name of datastore

Triggers: Execute show datastore Commandline interface.

SUCCEEDED_SHOW_DATASTORE

ID: AMCLI-5001

Level: INFO

Description: Show datastore succeeded.

Data: name of realm, name of datastore

Triggers: Execute show datastore Commandline interface.

FAILED_SHOW_DATASTORE

ID: AMCLI-5002

Level: INFO

Description: Failed to show datastore profile.

Data: name of realm, name of datastore, error message

Triggers: Execute show datastore Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_SET_SVC_ATTR_VALUES_REALM

ID: AMCLI-5200

Level: INFO

Description: Attempt to set attribute value to a service that is assigned to a realm.

Data: name of realm, name of service

Triggers: Execute set attribute values a service that is assigned to a to realm Commandline interface.

SUCCEED_SET_SVC_ATTR_VALUES_REALM

ID: AMCLI-5201

Level: INFO

Description: Attribute values is set to a service that is assigned to a realm.

Data: name of realm, name of service

Triggers: Execute set attribute values to a service that is assigned to a realm Commandline interface.

FAILED_SET_SVC_ATTR_VALUES_REALM

ID: AMCLI-5202

Level: INFO

Description: Unable to set attribute values to a service that is assigned to a realm.

Data: name of realm, name of service, error message

Triggers: Execute set attribute values to a service that is assigned to a realm Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_EMBEDDED_STATUS

ID: AMCLI-5103

Level: INFO

Description: Get Embedded Status.

Data: port number of embedded store

Triggers: Execute Embedded Status Commandline interface.

SUCCEEDED_EMBEDDED_STATUS

ID: AMCLI-5104

Level: INFO

Description: Embedded Status Successful.

Data: port number of embedded store

Triggers: Execute Embedded Status Commandline interface.

FAILED_EMBEDDED_STATUS

ID: AMCLI-5105

Level: INFO

Description: Failed to get embedded status.

Data: port number of embedded store, error message

Triggers: Execute Embedded Status Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_ADD_COT_MEMBER

ID: AMCLI-5106

Level: INFO

Description: Attempt to add a member to a Circle of Trust.

Data: realm, entity ID, circle of trust, protocol specification

Triggers: Execute add a member to a Circle of Trust Commandline interface.

SUCCEEDED_ADD_COT_MEMBER

ID: AMCLI-5107

Level: INFO

Description: Adding a member to a Circle of Trust succeeded.

Data: realm, entity ID, circle of trust, protocol specification

Triggers: Execute add a member to a Circle of Trust Commandline interface.

FAILED_ADD_COT_MEMBER

ID: AMCLI-5108

Level: INFO

Description: Failed to add a member to a circle of trust.

Data: realm, entity ID, circle of trust, protocol specification, error message

Triggers: Execute add a member to a Circle of Trust Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_DO_BULK_FEDERATION

ID: AMCLI-5109

Level: INFO

Description: Attempt to do bulk federation.

Data: metaAlias for local provider, Remote entity Id, File name of local to remote user Id mapping, Name of file that will be created by this sub command, protocol specification

Triggers: Execute Do Bulk Federation Commandline interface.

SUCCEEDED_DO_BULK_FEDERATION

ID: AMCLI-5110

Level: INFO

Description: Bulk Federation succeeded.

Data: metaAlias for local provider, Remote entity Id, File name of local to remote user Id mapping, Name of file that will be created by this sub command, protocol specification

Triggers: Execute Do Bulk Federation Commandline interface.

FAILED_DO_BULK_FEDERATION

ID: AMCLI-5111

Level: INFO

Description: Failed to do bulk federation.

Data: metaAlias for local provider, Remote entity Id, File name of local to remote user Id mapping, Name of file that will be created by this sub command, protocol specification, error message

Triggers: Execute Do Bulk Federation Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_CREATE_COT

ID: AMCLI-5112

Level: INFO

Description: Attempt to create Circle of Trust.

Data: Realm, Circle of Trust, Trusted Providers, Prefix URL for idp discovery reader and writer URL

Triggers: Execute Create Circle of Trust Commandline interface.

SUCCEEDED_CREATE_COT

ID: AMCLI-5113

Level: INFO

Description: Creating Circle of Trust succeeded.

Data: Realm, Circle of Trust, Trusted Providers, Prefix URL for idp discovery reader and writer URL

Triggers: Execute Create Circle of Trust Commandline interface.

FAILED_CREATE_COT

ID: AMCLI-5114

Level: INFO

Description: Failed to create Circle of Trust.

Data: Realm, Circle of Trust, Trusted Providers, Prefix URL for idp discovery reader and writer URL, error message

Triggers: Execute Create Circle of Trust Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_CREATE_METADATA_TEMPL

ID: AMCLI-5115

Level: INFO

Description: Attempt to create metadata template.

Data: Entity ID, file name for the standard metadata to be created, file name for the extended metadata to be created, metaAlias for hosted identity provider to be created, metaAlias for hosted service provider to be created, metaAlias for hosted attribute authority to be created, metaAlias for hosted attribute query provider to be created, metaAlias for hosted authentication authority to be created, metaAlias for policy decision point to be created, metaAlias for policy enforcement point to be created, metaAlias for hosted affiliation, protocol specification

Triggers: Execute Create MetaData Template Commandline interface.

SUCCEEDED_CREATE_METADATA_TEMPL

ID: AMCLI-5116

Level: INFO

Description: Creating MetaData Template succeeded.

Data: Entity ID, file name for the standard metadata to be created, file name for the extended metadata to be created, metaAlias for hosted identity provider to be created, metaAlias for hosted service provider to be created, metaAlias for hosted attribute authority to be created, metaAlias for hosted attribute query provider to be created, metaAlias for hosted authentication authority to be created, metaAlias for policy decision point to be created, metaAlias for policy enforcement point to be created, metaAlias for hosted affiliation, protocol specification

Triggers: Execute Create MetaData Template Commandline interface.

FAILED_CREATE_METADATA_TEMPL

ID: AMCLI-5117

Level: INFO

Description: Failed to create metaData template.

Data: Entity ID, protocol specification, error message

Triggers: Execute Create MetaData Template Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_DELETE_COT

ID: AMCLI-5118

Level: INFO

Description: Attempt to delete Circle of Trust.

Data: Realm, Circle of Trust

Triggers: Execute Delete Circle of Trust Commandline interface.

SUCCEEDED_DELETE_COT

ID: AMCLI-5119

Level: INFO

Description: Deleting Circle of Trust succeeded.

Data: Realm, Circle of Trust

Triggers: Execute Delete Circle of Trust Commandline interface.

FAILED_DELETE_COT

ID: AMCLI-5120

Level: INFO

Description: Failed to delete Circle of Trust.

Data: Realm, Circle of Trust, error message

Triggers: Execute Delete Circle of Trust Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_DELETE_ENTITY

ID: AMCLI-5121

Level: INFO

Description: Attempt to delete metadata.

Data: Realm, Entity ID, protocol specification

Triggers: Execute Delete Metadata Commandline interface.

SUCCEEDED_DELETE_ENTITY

ID: AMCLI-5122

Level: INFO

Description: Deleting Metadata succeeded.

Data: Realm, Entity ID, protocol specification

Triggers: Execute Delete Metadata Commandline interface.

FAILED_DELETE_ENTITY

ID: AMCLI-5123

Level: INFO

Description: Failed to delete metadata.

Data: Realm, Entity ID, protocol specification, error message

Triggers: Execute Delete Metadata Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_EXPORT_ENTITY

ID: AMCLI-5124

Level: INFO

Description: Attempt to export entity.

Data: Realm, Entity ID, Name of file to save the standard metadata XML, Name of file to save the extended metadata XML, protocol specification

Triggers: Execute export entity Commandline interface.

SUCCEEDED_EXPORT_ENTITY

ID: AMCLI-5125

Level: INFO

Description: Exporting entity succeeded.

Data: Realm, Entity ID, Name of file to save the standard metadata XML, Name of file to save the extended metadata XML, protocol specification

Triggers: Execute export entity Commandline interface.

FAILED_EXPORT_ENTITY

ID: AMCLI-5126

Level: INFO

Description: Failed to export entity.

Data: Realm, Entity ID, Name of file to save the standard metadata XML, Name of file to save the extended metadata XML, protocol specification, error message

Triggers: Execute export entity Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_IMPORT_BULK_FED_DATA

ID: AMCLI-5127

Level: INFO

Description: Attempt to import bulk federation data.

Data: metaAlias for local provider, File name of bulk federation data which is generated by this command, protocol specification

Triggers: Execute import bulk federation data Commandline interface.

SUCCEEDED_IMPORT_BULK_FED_DATA

ID: AMCLI-5128

Level: INFO

Description: Importing bulk federation data succeeded.

Data: metaAlias for local provider, File name of bulk federation data which is generated by this command, protocol specification

Triggers: Execute import bulk federation data Commandline interface.

FAILED_IMPORT_BULK_FED_DATA

ID: AMCLI-5129

Level: INFO

Description: Failed to import bulk federation data.

Data: metaAlias for local provider, File name of bulk federation data which is generated by this command, protocol specification, error message

Triggers: Execute import bulk federation data Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_IMPORT_ENTITY

ID: AMCLI-5130

Level: INFO

Description: Attempt to import entity.

Data: Realm where entity resides, file name for the standard metadata to be imported, file name for the extended entity configuration to be imported, name of the Circle of Trust this entity belongs, protocol specification

Triggers: Execute import entity Commandline interface.

SUCCEEDED_IMPORT_ENTITY

ID: AMCLI-5131

Level: INFO

Description: Importing entity succeeded.

Data: Realm where entity resides, file name for the standard metadata to be imported, file name for the extended entity configuration to be imported, name of the Circle of Trust this entity belongs, protocol specification

Triggers: Execute import entity Commandline interface.

FAILED_IMPORT_ENTITY

ID: AMCLI-5132

Level: INFO

Description: Failed to import entity.

Data: Realm where entity resides, file name for the standard metadata to be imported, file name for the extended entity configuration to be imported, name of the Circle of Trust this entity belongs, protocol specification, error message

Triggers: Execute import entity Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_LIST_COT_MEMBERS

ID: AMCLI-5133

Level: INFO

Description: Attempt to list members in a circle of trust.

Data: Realm, Circle of trust, protocol specification

Triggers: Execute list members in a circle of trust Commandline interface.

SUCCEEDED_LIST_COT_MEMBERS

ID: AMCLI-5134

Level: INFO

Description: Listing members in a circle of trust succeeded.

Data: Realm, Circle of trust, protocol specification

Triggers: Execute list members in a circle of trust Commandline interface.

FAILED_LIST_COT_MEMBERS

ID: AMCLI-5135

Level: INFO

Description: Failed to list members in a circle of trust.

Data: Realm, Circle of trust, protocol specification, error message

Triggers: Execute list members in a circle of trust Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_LIST_COTS

ID: AMCLI-5136

Level: INFO

Description: Attempt to list circles of trust.

Data: realm

Triggers: Execute list circles of trust Commandline interface.

SUCCEEDED_LIST_COTS

ID: AMCLI-5137

Level: INFO

Description: Listing circles of trust succeeded.

Data: realm

Triggers: Execute list circles of trust Commandline interface.

FAILED_LIST_COTS

ID: AMCLI-5138

Level: INFO

Description: Failed to list circles of trust.

Data: realm, error message

Triggers: Execute list circles of trust Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_LIST_ENTITIES

ID: AMCLI-5139

Level: INFO

Description: Attempt to list entities under a realm.

Data: realm, protocol specification

Triggers: Execute list entities under a realm Commandline interface.

SUCCEEDED_LIST_ENTITIES

ID: AMCLI-5140

Level: INFO

Description: Listing entities under a realm succeeded.

Data: realm, protocol specification

Triggers: Execute list entities under a realm Commandline interface.

FAILED_LIST_ENTITIES

ID: AMCLI-5141

Level: INFO

Description: Failed to list entities under a realm.

Data: realm, protocol specification, error message

Triggers: Execute list entities under a realm Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_REMOVE_COT_MEMBER

ID: AMCLI-5142

Level: INFO

Description: Attempt to remove a member from a circle of trust.

Data: Realm where circle of trust resides, Circle of trust, Entity ID, protocol specification

Triggers: Execute remove a member from a circle of trust Commandline interface.

SUCCEEDED_REMOVE_COT_MEMBER

ID: AMCLI-5143

Level: INFO

Description: Removing a member from a circle of trust successful.

Data: Realm where circle of trust resides, Circle of trust, Entity ID, protocol specification

Triggers: Execute remove a member from a circle of trust Commandline interface.

FAILED_REMOVE_COT_MEMBER

ID: AMCLI-5144

Level: INFO

Description: Failed to remove a member from a circle of trust.

Data: Realm where circle of trust resides, Circle of trust, Entity ID, protocol specification, error message

Triggers: Execute remove a member from a circle of trust Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_UPDATE_ENTITY_KEYINFO

ID: AMCLI-5145

Level: INFO

Description: Attempt to update XML signing and encryption key information in hosted entity metadata.

Data: Realm, Entity ID, Service provider signing certificate alias, Identity provider signing certificate alias, Service provider encryption certificate alias, Identity provider encryption certificate alias, protocol specification

Triggers: Execute Commandline interface.

SUCCEEDED_UPDATE_ENTITY_KEYINFO

ID: AMCLI-5146

Level: INFO

Description: Updating XML signing and encryption key information in hosted entity metadata succeeded.

Data: Realm, Entity ID, Service provider signing certificate alias, Identity provider signing certificate alias, Service provider encryption certificate alias, Identity provider encryption certificate alias

Triggers: Execute update XML signing and encryption key information in hosted entity metadata Commandline interface.

FAILED_UPDATE_ENTITY_KEYINFO

ID: AMCLI-5147

Level: INFO

Description: Failed to update XML signing and encryption key information in hosted entity metadata.

Data: Realm, Entity ID, Service provider signing certificate alias, Identity provider signing certificate alias, Service provider encryption certificate alias, Identity provider encryption certificate alias, error message

Triggers: Execute update XML signing and encryption key information in hosted entity metadata Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_CREATE_APPLICATION

ID: AMCLI-5500

Level: INFO

Description: Attempt to create application.

Data: Realm, Application name

Triggers: Execute create application Commandline interface.

SUCCEEDED_CREATE_APPLICATION

ID: AMCLI-5501

Level: INFO

Description: Create application succeeded.

Data: Realm, Application name

Triggers: Execute create application Commandline interface.

FAILED_CREATE_APPLICATION

ID: AMCLI-5502

Level: INFO

Description: Failed to create application.

Data: Realm, Application name, error message

Triggers: Execute create application Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_LIST_APPLICATIONS

ID: AMCLI-5510

Level: INFO

Description: Attempt to list applications in a realm.

Data: Realm

Triggers: Execute list applications Commandline interface.

SUCCEEDED_LIST_APPLICATIONS

ID: AMCLI-5511

Level: INFO

Description: List applications in a realm succeeded.

Data: Realm

Triggers: Execute list applications Commandline interface.

FAILED_LIST_APPLICATIONS

ID: AMCLI-5512

Level: INFO

Description: Failed to list applications.

Data: Realm, error message

Triggers: Execute list applications Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_LIST_APPLICATION_TYPES

ID: AMCLI-5520

Level: INFO

Description: Attempt to list application types.

Triggers: Execute list application types Commandline interface.

SUCCEEDED_LIST_APPLICATION_TYPES

ID: AMCLI-5521

Level: INFO

Description: List application types succeeded.

Triggers: Execute list application types Commandline interface.

FAILED_LIST_APPLICATION_TYPES

ID: AMCLI-5522

Level: INFO

Description: Failed to list application types.

Data: error message

Triggers: Execute list application types Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_SHOW_APPLICATION

ID: AMCLI-5530

Level: INFO

Description: Attempt to show application attributes.

Data: Realm, Application Name

Triggers: Execute show application Commandline interface.

SUCCEEDED_SHOW_APPLICATION

ID: AMCLI-5531

Level: INFO

Description: Attributes of application is displayed succeeded.

Data: Realm, Application Name

Triggers: Execute show application Commandline interface.

FAILED_SHOW_APPLICATION

ID: AMCLI-5532

Level: INFO

Description: Failed to show application attributes.

Data: Realm, Application Name, error message

Triggers: Execute show application Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_SET_APPLICATION

ID: AMCLI-5540

Level: INFO

Description: Attempt to set application attributes.

Data: Realm, Application Name

Triggers: Execute set application attributes Commandline interface.

SUCCEEDED_SET_APPLICATION

ID: AMCLI-5541

Level: INFO

Description: Attributes of application is modified succeeded.

Data: Realm, Application Name

Triggers: Execute set application attributes Commandline interface.

FAILED_SET_APPLICATION

ID: AMCLI-5542

Level: INFO

Description: Failed to set application attributes.

Data: Realm, Application Name, error message

Triggers: Execute set application attributes Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_DELETE_APPLICATIONS

ID: AMCLI-5550

Level: INFO

Description: Attempt to delete applications.

Data: Realm

Triggers: Execute delete applications Commandline interface.

SUCCEEDED_DELETE_APPLICATIONS

ID: AMCLI-5551

Level: INFO

Description: Application are deleted.

Data: Realm

Triggers: Execute delete applications Commandline interface.

FAILED_DELETE_APPLICATIONS

ID: AMCLI-5552

Level: INFO

Description: Failed to delete applications.

Data: Realm, error message

Triggers: Execute delete applications Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_SHOW_APPLICATION_TYPE

ID: AMCLI-5553

Level: INFO

Description: Attempt to show application type details.

Data: Application Type name

Triggers: Execute show application type Commandline interface.

SUCCEEDED_SHOW_APPLICATION_TYPE

ID: AMCLI-5554

Level: INFO

Description: Show application type details succeeded.

Data: Application Type name

Triggers: Execute show application type Commandline interface.

ATTEMPT_DELETE_APPLICATION_TYPES

ID: AMCLI-5555

Level: INFO

Description: Attempt to delete application types.

Data: Application Type names

Triggers: Execute delete application types Commandline interface.

SUCCEEDED_DELETE_APPLICATION_TYPES

ID: AMCLI-5556

Level: INFO

Description: Delete application types succeeded.

Data: Application Type names

Triggers: Execute delete application types Commandline interface.

FAILED_DELETE_APPLICATION_TYPES

ID: AMCLI-5557

Level: INFO

Description: Delete application types failed.

Data: Application Type names, error message

Triggers: Execute delete application types Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_CREATE_APPLICATION_TYPE

ID: AMCLI-5558

Level: INFO

Description: Attempt to create application type.

Data: Application Type name

Triggers: Execute create application type Commandline interface.

SUCCEEDED_CREATE_APPLICATION_TYPE

ID: AMCLI-5559

Level: INFO

Description: Create application type succeeded.

Data: Application Type name

Triggers: Execute create application type Commandline interface.

FAILED_CREATE_APPLICATION_TYPE

ID: AMCLI-5560

Level: INFO

Description: Failed to create application type.

Data: Application Type name, error message

Triggers: Execute create application type Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_SHOW_ENTITLEMENT_SVC

ID: AMCLI-5600

Level: INFO

Description: Attempt to show entitlement service configuration.

Triggers: Execute show entitlement service configuration Commandline interface.

SUCCEEDED_SHOW_ENTITLEMENT_SVC

ID: AMCLI-5601

Level: INFO

Description: Entitlement service configuration is displayed.

Triggers: Execute show entitlement service configuration Commandline interface.

FAILED_SHOW_ENTITLEMENT_SVC

ID: AMCLI-5602

Level: INFO

Description: Failed to display entitlement service configuration.

Data: error message

Triggers: Execute show entitlement service configuration Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_MODIFY_ENTITLEMENT_SVC

ID: AMCLI-5610

Level: INFO

Description: Attempt to modify entitlement service configuration.

Triggers: Execute set entitlement service configuration Commandline interface.

SUCCEEDED_MODIFY_ENTITLEMENT_SVC

ID: AMCLI-5611

Level: INFO

Description: Entitlement service configuration is modified.

Triggers: Execute set entitlement service configuration Commandline interface.

FAILED_MODIFY_ENTITLEMENT_SVC

ID: AMCLI-5612

Level: INFO

Description: Failed to modify entitlement service configuration.

Data: error message

Triggers: Execute set entitlement service configuration Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_CREATE_APPLICATION_PRIVILEGE

ID: AMCLI-6010

Level: INFO

Description: Attempt to create application privilege.

Data: realm, application privilege name

Triggers: Execute create application privilege Commandline interface.

SUCCEEDED_CREATE_APPLICATION_PRIVILEGE

ID: AMCLI-6011

Level: INFO

Description: Application privilege is created.

Data: realm, application privilege name

Triggers: Execute create application privilege Commandline interface.

FAILED_CREATE_APPLICATION_PRIVILEGE

ID: AMCLI-6012

Level: INFO

Description: Failed to create application privilege.

Data: realm, application privilege name, error message

Triggers: Execute create application privilege Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_DELETE_APPLICATION_PRIVILEGE

ID: AMCLI-6020

Level: INFO

Description: Attempt to delete application privilege.

Data: realm, application privilege name

Triggers: Execute delete application privilege Commandline interface.

SUCCEEDED_DELETE_APPLICATION_PRIVILEGE

ID: AMCLI-6021

Level: INFO

Description: Application privilege is deleted.

Data: realm, application privilege name

Triggers: Execute delete application privilege Commandline interface.

FAILED_DELETE_APPLICATION_PRIVILEGE

ID: AMCLI-6022

Level: INFO

Description: Failed to delete application privilege.

Data: realm, application privilege name, error message

Triggers: Execute delete application privilege Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_SHOW_APPLICATION_PRIVILEGE

ID: AMCLI-6020

Level: INFO

Description: Attempt to show application privilege.

Data: realm, application privilege name

Triggers: Execute show application privilege Commandline interface.

SUCCEEDED_SHOW_APPLICATION_PRIVILEGE

ID: AMCLI-6021

Level: INFO

Description: Application privilege is displayed.

Data: realm, application privilege name

Triggers: Execute show application privilege Commandline interface.

FAILED_SHOW_APPLICATION_PRIVILEGE

ID: AMCLI-6022

Level: INFO

Description: Failed to show application privilege.

Data: realm, application privilege name, error message

Triggers: Execute show application privilege Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_LIST_APPLICATION_PRIVILEGES

ID: AMCLI-6030

Level: INFO

Description: Attempt to list application privileges in a realm.

Data: realm

Triggers: Execute list application privileges Commandline interface.

SUCCEEDED_LIST_APPLICATION_PRIVILEGES

ID: AMCLI-6031

Level: INFO

Description: Application privileges are displayed.

Data: realm

Triggers: Execute list application privileges Commandline interface.

FAILED_LIST_APPLICATION_PRIVILEGES

ID: AMCLI-6032

Level: INFO

Description: Failed to list application privileges.

Data: realm, error message

Triggers: Execute list application privileges Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_UPDATE_APPLICATION_PRIVILEGE

ID: AMCLI-6040

Level: INFO

Description: Attempt to update application privilege.

Data: realm, application privilege name

Triggers: Execute update application privilege Commandline interface.

SUCCEEDED_UPDATE_APPLICATION_PRIVILEGE

ID: AMCLI-6041

Level: INFO

Description: Application privilege is updated.

Data: realm, application privilege name

Triggers: Execute update application privilege Commandline interface.

FAILED_UPDATE_APPLICATION_PRIVILEGE

ID: AMCLI-6042

Level: INFO

Description: Failed to update application privilege.

Data: realm, application privilege name, error message

Triggers: Execute update application privileges Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_ADD_PLUGIN_SCHEMA

ID: AMCLI-6043

Level: INFO

Description: Attempt to add Plug-in schema.

Data: name of service, name of interface, name of plugin, name of i18n key, name of i18n name, name of class

Triggers: Execute add Plug-in schema Commandline interface.

SUCCEED_ADD_PLUGIN_SCHEMA

ID: AMCLI-6044

Level: INFO

Description: Added Plug-in schema.

Data: name of service, name of plugin

Triggers: Execute add Plug-in schema Commandline interface.

FAILED_ADD_PLUGIN_SCHEMA

ID: AMCLI-6045

Level: INFO

Description: Failed to add Plug-in schema.

Data: name of service, name of plugin, error message

Triggers: Execute add Plug-in schema Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_REMOVE_PLUGIN_SCHEMA

ID: AMCLI-6046

Level: INFO

Description: Attempt to remove Plug-in schema.

Data: name of service, name of interface, name of plugin, name of i18n key, name of i18n name, name of class

Triggers: Execute remove Plug-in schema Commandline interface.

SUCCEED_REMOVE_PLUGIN_SCHEMA

ID: AMCLI-6047

Level: INFO

Description: Removed Plug-in schema.

Data: name of service, name of plugin

Triggers: Execute remove Plug-in schema Commandline interface.

FAILED_REMOVE_PLUGIN_SCHEMA

ID: AMCLI-6048

Level: INFO

Description: Failed to remove Plug-in schema.

Data: name of service, name of plugin, error message

Triggers: Execute remove Plug-in schema Commandline interface.

Actions: Look under debug file for more information.

SUCCEED_SET_SITE_ID

ID: AMCLI-6049

Level: INFO

Description: Site ID is set.

Data: name of site, id of site

Triggers: Execute set site ID Commandline interface.

FAILED_SET_SITE_ID

ID: AMCLI-6050

Level: INFO

Description: Unable to set site ID.

Data: name of site, site ID, error message

Triggers: Execute set site ID Commandline interface.

Actions: Look under debug file for more information.

FAILED_START_RECORD

ID: AMCLI-6051

Level: INFO

Description: Unable to start the record.

Data: Server name, Json record, error message

Triggers: Execute start record Commandline interface.

Actions: Look under debug file for more information.

FAILED_STATUS_RECORD

ID: AMCLI-6052

Level: INFO

Description: Unable to get the status of the recording

Data: Server name, error message

Triggers: Execute status record Commandline interface.

Actions: Look under debug file for more information.

FAILED_STOP_RECORD

ID: AMCLI-6054

Level: INFO

Description: Recording can't be stopped

Data: Server name, error message

Triggers: Execute stop record Commandline interface.

Actions: Look under debug file for more information.

SUCCESS_START_RECORD

ID: AMCLI-6055

Level: INFO

Description: Start recording

Data: Server name, Json record, Json result

Triggers: Execute start record Commandline interface.

Actions: Look under debug file for more information.

SUCCESS_STATUS_RECORD

ID: AMCLI-6056

Level: INFO

Description: Get the status of the record with success

Data: Server name, Json result

Triggers: Execute status record Commandline interface.

Actions: Look under debug file for more information.

SUCCESS_STOP_RECORD

ID: AMCLI-6057

Level: INFO

Description: Stop recording

Data: Server name, Json result

Triggers: Execute stop record Commandline interface.

Actions: Look under debug file for more information.

ATTEMPT_STOP_RECORD

ID: AMCLI-6058

Level: INFO

Description: Attempt to stop recording.

Data: Server name

Triggers: Stop recording OpenAM.

ATTEMPT_STATUS_RECORD

ID: AMCLI-6059

Level: INFO

Description: Attempt to get the status of the recording.

Data: Server name

Triggers: Get the status of the current record.

ATTEMPT_START_RECORD

ID: AMCLI-6060

Level: INFO

Description: Attempt to start recording.

Data: Server name, Json record, Json result

Triggers: Start record.

RESOURCE_READ_FAILED

ID: AMCLI-6100

Level: INFO

Description: Failed to read resource.

Data: Resource Id, Resource type, Http code

Triggers: Attempting to read resource to determine whether to create or update.

RESOURCE_UPDATE_SUCCESS

ID: AMCLI-6101

Level: INFO

Description: Successfully updated resource.

Data: Resource Id, Resource type

Triggers: Attempting to update an existing resource.

RESOURCE_UPDATE_FAILED

ID: AMCLI-6102

Level: INFO

Description: Failed to update resource.

Data: Resource Id, Resource type, Http code

Triggers: Attempting to update an existing resource.

RESOURCE_CREATE_SUCCESS

ID: AMCLI-6103

Level: INFO

Description: Successfully created resource.

Data: Resource Id, Resource type

Triggers: Attempting to create a new resource.

RESOURCE_CREATE_FAILED

ID: AMCLI-6104

Level: INFO

Description: Failed to create resource.

Data: Resource Id, Resource type, Http code

Triggers: Attempting to create a new resource.

POLICY_EXPORT_SUCCESS

ID: AMCLI-6105

Level: INFO

Description: Successfully exported policy model resources.

Data: Realm, Exported File

Triggers: Executes export resource Commandline interface.

OpenAM logs the following CONSOLE messages.

ATTEMPT_IDENTITY_CREATION

ID: CONSOLE-1

Level: INFO

Description: Attempt to create Identity

Data: identity name, identity type, realm name

Triggers: Click on create button in Realm Creation Page.

IDENTITY_CREATED

ID: CONSOLE-2

Level: INFO

Description: Creation of Identity succeeded.

Data: identity name, identity type, realm name

Triggers: Click on create button in Realm Creation Page.

SSO_EXCEPTION_IDENTITY_CREATION

ID: CONSOLE-3

Level: SEVERE

Description: Creation of Identity failed

Data: identity name, identity type, realm name, error message

Triggers: Unable to create an identity under a realm. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.

Actions: Look under data store log for more information.

IDM_EXCEPTION_IDENTITY_CREATION

ID: CONSOLE-4

Level: SEVERE

Description: Creation of Identity failed

Data: identity name, identity type, realm name, error message

Triggers: Unable to create an identity under a realm due to data store error.

Actions: Look under data store log for more information.

ATTEMPT_SEARCH_IDENTITY

ID: CONSOLE-11

Level: INFO

Description: Attempt to search for Identities

Data: base realm, identity type, search pattern, search size limit, search time limit

Triggers: Click on Search button in identity search view.

SUCCEED_SEARCH_IDENTITY

ID: CONSOLE-12

Level: INFO

Description: Searching for Identities succeeded

Data: base realm, identity type, search pattern, search size limit, search time limit

Triggers: Click on Search button in identity search view.

SSO_EXCEPTION_SEARCH_IDENTITY

ID: CONSOLE-13

Level: SEVERE

Description: Searching for identities failed

Data: identity name, identity type, realm name, error message

Triggers: Unable to perform search operation on identities under a realm. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.

Actions: Look under data store log for more information.

IDM_EXCEPTION_SEARCH_IDENTITY

ID: CONSOLE-14

Level: SEVERE

Description: Searching for identities failed

Data: identity name, identity type, realm name, error message

Triggers: Unable to perform search operation on identities under a realm due to data store error.

Actions: Look under data store log for more information.

ATTEMPT_READ_IDENTITY_ATTRIBUTE_VALUE

ID: CONSOLE-21

Level: INFO

Description: Attempt to read attribute values of an identity

Data: identity name, name of attributes

Triggers: View identity profile view.

SUCCEED_READ_IDENTITY_ATTRIBUTE_VALUE

ID: CONSOLE-22

Level: INFO

Description: Reading of attribute values of an identity succeeded

Data: identity name, name of attributes

Triggers: View identity profile view.

SSO_EXCEPTION_READ_IDENTITY_ATTRIBUTE_VALUE

ID: CONSOLE-23

Level: SEVERE

Description: Reading of attribute values of an identity failed

Data: identity name, name of attributes, error message

Triggers: Unable to read attribute values of an identity. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.

Actions: Look under data store log for more information.

IDM_EXCEPTION_READ_IDENTITY_ATTRIBUTE_VALUE

ID: CONSOLE-24

Level: SEVERE

Description: Reading of attribute values of an identity failed

Data: identity name, name of attributes, error message

Triggers: Unable to read attribute values of an identity due to data store error.

Actions: Look under data store log for more information.

SMS_EXCEPTION_READ_IDENTITY_ATTRIBUTE_VALUE

ID: CONSOLE-25

Level: SEVERE

Description: Reading of attribute values of an identity failed

Data: identity name, name of attributes, error message

Triggers: Unable to read attribute values of an identity due to exception service manager API.

Actions: Look under service manage log for more information.

ATTEMPT_MODIFY_IDENTITY_ATTRIBUTE_VALUE

ID: CONSOLE-31

Level: INFO

Description: Attempt to modify attribute values of an identity

Data: identity name, name of attributes

Triggers: Click on Save button in identity profile view.

SUCCEED_MODIFY_IDENTITY_ATTRIBUTE_VALUE

ID: CONSOLE-32

Level: INFO

Description: Modification of attribute values of an identity succeeded

Data: identity name, name of attributes

Triggers: Click on Save button in identity profile view.

SSO_EXCEPTION_MODIFY_IDENTITY_ATTRIBUTE_VALUE

ID: CONSOLE-33

Level: SEVERE

Description: Modification of attribute values of an identity failed

Data: identity name, name of attributes, error message

Triggers: Unable to modify attribute values of an identity. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.

Actions: Look under data store log for more information.

IDM_EXCEPTION_MODIFY_IDENTITY_ATTRIBUTE_VALUE

ID: CONSOLE-34

Level: SEVERE

Description: Modification of attribute values of an identity failed

Data: identity name, name of attributes, error message

Triggers: Unable to modify attribute values of an identity due to data store error.

Actions: Look under data store log for more information.

ATTEMPT_DELETE_IDENTITY

ID: CONSOLE-41

Level: INFO

Description: Attempt to delete identities

Data: realm name, name of identities to be deleted

Triggers: Click on Delete button in identity search view.

SUCCEED_DELETE_IDENTITY

ID: CONSOLE-42

Level: INFO

Description: Deletion of identities succeeded

Data: realm name, name of identities to be deleted

Triggers: Click on Delete button in identity search view.

SSO_EXCEPTION_DELETE_IDENTITY

ID: CONSOLE-43

Level: SEVERE

Description: Deletion of identities failed

Data: realm name, name of identities to be deleted, error message

Triggers: Unable to delete identities. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.

Actions: Look under data store log for more information.

IDM_EXCEPTION_DELETE_IDENTITY

ID: CONSOLE-44

Level: SEVERE

Description: Deletion of identities failed

Data: realm name, name of identities to be deleted, error message

Triggers: Unable to delete identities due to data store error.

Actions: Look under data store log for more information.

ATTEMPT_READ_IDENTITY_MEMBERSHIP

ID: CONSOLE-51

Level: INFO

Description: Attempt to read identity's memberships information

Data: name of identity, membership identity type

Triggers: View membership page of an identity.

SUCCEED_READ_IDENTITY_MEMBERSHIP

ID: CONSOLE-52

Level: INFO

Description: Reading of identity's memberships information succeeded

Data: name of identity, membership identity type

Triggers: View membership page of an identity.

SSO_EXCEPTION_READ_IDENTITY_MEMBERSHIP

ID: CONSOLE-53

Level: SEVERE

Description: Reading of identity's memberships information failed.

Data: name of identity, membership identity type, error message

Triggers: Unable to read identity's memberships information. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.

Actions: Look under data store log for more information.

IDM_EXCEPTION_READ_IDENTITY_MEMBERSHIP

ID: CONSOLE-54

Level: SEVERE

Description: Reading of identity's memberships information failed.

Data: name of identity, membership identity type, error message

Triggers: Unable to read identity's memberships information due to data store error.

Actions: Look under data store log for more information.

ATTEMPT_READ_IDENTITY_MEMBER

ID: CONSOLE-61

Level: INFO

Description: Attempt to read identity's members information

Data: name of identity, members identity type

Triggers: View members page of an identity.

SUCCEED_READ_IDENTITY_MEMBER

ID: CONSOLE-62

Level: INFO

Description: Reading of identity's members information succeeded

Data: name of identity, members identity type

Triggers: View members page of an identity.

SSO_EXCEPTION_READ_IDENTITY_MEMBER

ID: CONSOLE-63

Level: SEVERE

Description: Reading of identity's members information failed.

Data: name of identity, member identity type, error message

Triggers: Unable to read identity's members information. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.

Actions: Look under data store log for more information.

IDM_EXCEPTION_READ_IDENTITY_MEMBER

ID: CONSOLE-64

Level: SEVERE

Description: Reading of identity's members information failed.

Data: name of identity, member identity type, error message

Triggers: Unable to read identity's members information due to data store error.

Actions: Look under data store log for more information.

ATTEMPT_ADD_IDENTITY_MEMBER

ID: CONSOLE-71

Level: INFO

Description: Attempt to add member to an identity

Data: name of identity, name of identity to be added.

Triggers: Select members to be added to an identity.

SUCCEED_ADD_IDENTITY_MEMBER

ID: CONSOLE-72

Level: INFO

Description: Addition of member to an identity succeeded

Data: name of identity, name of identity added.

Triggers: Select members to be added to an identity.

SSO_EXCEPTION_ADD_IDENTITY_MEMBER

ID: CONSOLE-73

Level: SEVERE

Description: Addition of member to an identity failed.

Data: name of identity, name of identity to be added., error message

Triggers: Unable to add member to an identity. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.

Actions: Look under data store log for more information.

IDM_EXCEPTION_ADD_IDENTITY_MEMBER

ID: CONSOLE-74

Level: SEVERE

Description: Addition of member to an identity failed.

Data: name of identity, name of identity to be added., error message

Triggers: Unable to add member to an identity due to data store error.

Actions: Look under data store log for more information.

ATTEMPT_REMOVE_IDENTITY_MEMBER

ID: CONSOLE-81

Level: INFO

Description: Attempt to remove member from an identity

Data: name of identity, name of identity to be removed.

Triggers: Select members to be removed from an identity.

SUCCEED_REMOVE_IDENTITY_MEMBER

ID: CONSOLE-82

Level: INFO

Description: Removal of member from an identity succeeded

Data: name of identity, name of identity removed.

Triggers: Select members to be removed from an identity.

SSO_EXCEPTION_REMOVE_IDENTITY_MEMBER

ID: CONSOLE-83

Level: SEVERE

Description: Removal of member to an identity failed.

Data: name of identity, name of identity to be removed., error message

Triggers: Unable to remove member from an identity. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.

Actions: Look under data store log for more information.

IDM_EXCEPTION_REMOVE_IDENTITY_MEMBER

ID: CONSOLE-84

Level: SEVERE

Description: Removal of member from an identity failed.

Data: name of identity, name of identity to be removed., error message

Triggers: Unable to remove member to an identity due to data store error.

Actions: Look under data store log for more information.

ATTEMPT_READ_IDENTITY_ASSIGNED_SERVICE

ID: CONSOLE-91

Level: INFO

Description: Attempt to read assigned service names of an identity

Data: name of identity

Triggers: Click on Add button in service assignment view of an identity.

SUCCEED_READ_IDENTITY_ASSIGNED_SERVICE

ID: CONSOLE-92

Level: INFO

Description: Reading assigned service names of an identity succeeded

Data: name of identity

Triggers: Click on Add button in service assignment view of an identity.

SSO_EXCEPTION_READ_IDENTITY_ASSIGNED_SERVICE

ID: CONSOLE-93

Level: SEVERE

Description: Reading assigned service names of an identity failed.

Data: name of identity, error message

Triggers: Unable to read assigned service names of an identity. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.

Actions: Look under data store log for more information.

IDM_EXCEPTION_READ_IDENTITY_ASSIGNED_SERVICE

ID: CONSOLE-94

Level: SEVERE

Description: Reading assigned service names of an identity failed.

Data: name of identity, error message

Triggers: Unable to read assigned service names of an identity due to data store error.

Actions: Look under data store log for more information.

ATTEMPT_READ_IDENTITY_ASSIGNABLE_SERVICE

ID: CONSOLE-101

Level: INFO

Description: Attempt to read assignable service names of an identity

Data: name of identity

Triggers: View the services page of an identity.

SUCCEED_READ_IDENTITY_ASSIGNABLE_SERVICE

ID: CONSOLE-102

Level: INFO

Description: Reading assignable service names of an identity succeeded

Data: name of identity

Triggers: View the services page of an identity.

SSO_EXCEPTION_READ_IDENTITY_ASSIGNABLE_SERVICE

ID: CONSOLE-103

Level: SEVERE

Description: Reading assignable service names of an identity failed.

Data: name of identity, error message

Triggers: Unable to read assignable service names of an identity. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.

Actions: Look under data store log for more information.

IDM_EXCEPTION_READ_IDENTITY_ASSIGNABLE_SERVICE

ID: CONSOLE-104

Level: SEVERE

Description: Reading assignable service names of an identity failed.

Data: name of identity, error message

Triggers: Unable to read assignable service names of an identity due to data store error.

Actions: Look under data store log for more information.

ATTEMPT_IDENTITY_ASSIGN_SERVICE

ID: CONSOLE-111

Level: INFO

Description: Attempt to assign a service to an identity

Data: name of identity, name of service

Triggers: Click Add button of service view of an identity.

SUCCEED_IDENTITY_ASSIGN_SERVICE

ID: CONSOLE-112

Level: INFO

Description: Assignment of service to an identity succeeded

Data: name of identity, name of service

Triggers: Click Add button of service view of an identity.

SSO_EXCEPTION_IDENTITY_ASSIGN_SERVICE

ID: CONSOLE-113

Level: SEVERE

Description: Assignment of service to an identity failed.

Data: name of identity, name of service, error message

Triggers: Unable to assign service to an identity. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.

Actions: Look under data store log for more information.

IDM_EXCEPTION_IDENTITY_ASSIGN_SERVICE

ID: CONSOLE-114

Level: SEVERE

Description: Assignment of service to an identity failed.

Data: name of identity, name of service, error message

Triggers: Unable to assign service to an identity due to data store error.

Actions: Look under data store log for more information.

ATTEMPT_IDENTITY_UNASSIGN_SERVICE

ID: CONSOLE-121

Level: INFO

Description: Attempt to unassign a service from an identity

Data: name of identity, name of service

Triggers: Click Remove button in service view of an identity.

SUCCEED_IDENTITY_UNASSIGN_SERVICE

ID: CONSOLE-122

Level: INFO

Description: Unassignment of service to an identity succeeded

Data: name of identity, name of service

Triggers: Click Remove button in service view of an identity.

SSO_EXCEPTION_IDENTITY_UNASSIGN_SERVICE

ID: CONSOLE-123

Level: SEVERE

Description: Unassignment of service from an identity failed.

Data: name of identity, name of service, error message

Triggers: Unable to unassign service from an identity. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.

Actions: Look under data store log for more information.

IDM_EXCEPTION_IDENTITY_UNASSIGN_SERVICE

ID: CONSOLE-124

Level: SEVERE

Description: Unassignment of service from an identity failed.

Data: name of identity, name of service, error message

Triggers: Unable to unassign service from an identity due to data store error.

Actions: Look under data store log for more information.

ATTEMPT_IDENTITY_READ_SERVICE_ATTRIBUTE_VALUES

ID: CONSOLE-131

Level: INFO

Description: Attempt to read service attribute values of an identity

Data: name of identity, name of service

Triggers: View service profile view of an identity.

SUCCEED_IDENTITY_READ_SERVICE_ATTRIBUTE_VALUES

ID: CONSOLE-132

Level: INFO

Description: Reading of service attribute values of an identity succeeded

Data: name of identity, name of service

Triggers: View service profile view of an identity.

SSO_EXCEPTION_IDENTITY_READ_SERVICE_ATTRIBUTE_VALUES

ID: CONSOLE-133

Level: SEVERE

Description: Reading of service attribute values of an identity failed.

Data: name of identity, name of service, error message

Triggers: Unable to read service attribute values of an identity. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation

Actions: Look under data store log for more information.

IDM_EXCEPTION_IDENTITY_READ_SERVICE_ATTRIBUTE_VALUES

ID: CONSOLE-134

Level: SEVERE

Description: Reading of service attribute values of an identity failed.

Data: name of identity, name of service, error message

Triggers: Unable to read service attribute values of an identity due to data store error.

Actions: Look under data store log for more information.

ATTEMPT_IDENTITY_WRITE_SERVICE_ATTRIBUTE_VALUES

ID: CONSOLE-141

Level: INFO

Description: Attempt to write service attribute values to an identity

Data: name of identity, name of service

Triggers: Click on Save button in service profile view of an identity.

SUCCEED_IDENTITY_WRITE_SERVICE_ATTRIBUTE_VALUES

ID: CONSOLE-142

Level: INFO

Description: Writing of service attribute values to an identity succeeded

Data: name of identity, name of service

Triggers: Click on Save button in service profile view of an identity.

SSO_EXCEPTION_IDENTITY_WRITE_SERVICE_ATTRIBUTE_VALUES

ID: CONSOLE-143

Level: SEVERE

Description: Writing of service attribute values to an identity failed.

Data: name of identity, name of service, error message

Triggers: Unable to write service attribute values to an identity. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.

Actions: Look under data store log for more information.

IDM_EXCEPTION_IDENTITY_WRITE_SERVICE_ATTRIBUTE_VALUES

ID: CONSOLE-144

Level: SEVERE

Description: Writing of service attribute values to an identity failed.

Data: name of identity, name of service, error message

Triggers: Unable to write service attribute values to an identity due to data store error.

Actions: Look under data store log for more information.

ATTEMPT_READ_ALL_GLOBAL_DEFAULT_ATTRIBUTE_VALUES

ID: CONSOLE-201

Level: INFO

Description: Attempt to read all global service default attribute values

Data: name of service

Triggers: View global configuration view of a service.

SUCCEED_READ_ALL_GLOBAL_DEFAULT_ATTRIBUTE_VALUES

ID: CONSOLE-202

Level: INFO

Description: Reading of all global service default attribute values succeeded

Data: name of service

Triggers: View global configuration view of a service.

ATTEMPT_READ_GLOBAL_DEFAULT_ATTRIBUTE_VALUES

ID: CONSOLE-203

Level: INFO

Description: Attempt to read global service default attribute values

Data: name of service, name of attribute

Triggers: View global configuration view of a service.

SUCCEED_READ_GLOBAL_DEFAULT_ATTRIBUTE_VALUES

ID: CONSOLE-204

Level: INFO

Description: Reading of global service default attribute values succeeded

Data: name of service, name of attribute

Triggers: View global configuration view of a service.

FAILED_READ_GLOBAL_DEFAULT_ATTRIBUTE_VALUES

ID: CONSOLE-205

Level: INFO

Description: Reading of global service default attribute values failed

Data: name of service, name of attribute

Triggers: View global configuration view of a service.

Actions: Look under service management log for more information.

ATTEMPT_WRITE_GLOBAL_DEFAULT_ATTRIBUTE_VALUES

ID: CONSOLE-211

Level: INFO

Description: Attempt to write global service default attribute values

Data: name of service, name of attribute

Triggers: Click on Save button in global configuration view of a service.

SUCCEED_WRITE_GLOBAL_DEFAULT_ATTRIBUTE_VALUES

ID: CONSOLE-212

Level: INFO

Description: Writing of global service default attribute values succeeded

Data: name of service, name of attribute

Triggers: Click on Save button in global configuration view of a service.

SSO_EXCEPTION_WRITE_GLOBAL_DEFAULT_ATTRIBUTE_VALUES

ID: CONSOLE-213

Level: SEVERE

Description: Writing of global service default attribute values failed.

Data: name of service, name of attribute, error message

Triggers: Unable to write global service default attribute values. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.

Actions: Look under service management log for more information.

SMS_EXCEPTION_WRITE_GLOBAL_DEFAULT_ATTRIBUTE_VALUES

ID: CONSOLE-214

Level: SEVERE

Description: Writing of global service default attribute values failed.

Data: name of service, name of attribute, error message

Triggers: Unable to write service default attribute values due to service management error.

Actions: Look under service management log for more information.

ATTEMPT_READ_GLOBAL_SUB_CONFIGURATION_NAMES

ID: CONSOLE-221

Level: INFO

Description: Attempt to get sub configuration names

Data: name of service, name of base global sub configuration

Triggers: View a global service view of which its service has sub schema.

SUCCEED_READ_GLOBAL_SUB_CONFIGURATION_NAMES

ID: CONSOLE-222

Level: INFO

Description: Reading of global sub configuration names succeeded

Data: name of service, name of base global sub configuration

Triggers: View a global service view of which its service has sub schema.

SSO_EXCEPTION_READ_GLOBAL_SUB_CONFIGURATION_NAMES

ID: CONSOLE-223

Level: SEVERE

Description: Reading of global sub configuration names failed.

Data: name of service, name of base global sub configuration, error message

Triggers: Unable to get global sub configuration names. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.

Actions: Look under service management log for more information.

SMS_EXCEPTION_READ_GLOBAL_SUB_CONFIGURATION_NAMES

ID: CONSOLE-224

Level: SEVERE

Description: Reading of global sub configuration names failed.

Data: name of service, name of base global sub configuration, error message

Triggers: Unable to get global sub configuration names due to service management error.

Actions: Look under service management log for more information.

ATTEMPT_DELETE_GLOBAL_SUB_CONFIGURATION

ID: CONSOLE-231

Level: INFO

Description: Attempt to delete sub configuration

Data: name of service, name of base global sub configuration, name of sub configuration to be deleted

Triggers: Click on delete selected button in global service profile view.

SUCCEED_DELETE_GLOBAL_SUB_CONFIGURATION

ID: CONSOLE-232

Level: INFO

Description: Deletion of sub configuration succeeded

Data: name of service, name of base global sub configuration, name of sub configuration to be deleted

Triggers: Click on delete selected button in global service profile view.

SSO_EXCEPTION_DELETE_GLOBAL_SUB_CONFIGURATION

ID: CONSOLE-233

Level: SEVERE

Description: Deletion of sub configuration failed.

Data: name of service, name of base global sub configuration, name of sub configuration to be deleted, error message

Triggers: Unable to delete sub configuration. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.

Actions: Look under service management log for more information.

SMS_EXCEPTION_DELETE_GLOBAL_SUB_CONFIGURATION

ID: CONSOLE-234

Level: SEVERE

Description: Deletion of sub configuration failed.

Data: name of service, name of base global sub configuration, name of sub configuration to be deleted, error message

Triggers: Unable to delete sub configuration due to service management error.

Actions: Look under service management log for more information.

ATTEMPT_CREATE_GLOBAL_SUB_CONFIGURATION

ID: CONSOLE-241

Level: INFO

Description: Attempt to create sub configuration

Data: name of service, name of base global sub configuration, name of sub configuration to be created, name of sub schema to be created

Triggers: Click on add button in create sub configuration view.

SUCCEED_CREATE_GLOBAL_SUB_CONFIGURATION

ID: CONSOLE-242

Level: INFO

Description: Creation of sub configuration succeeded

Data: name of service, name of base global sub configuration, name of sub configuration to be created, name of sub schema to be created

Triggers: Click on add button in create sub configuration view.

SSO_EXCEPTION_CREATE_GLOBAL_SUB_CONFIGURATION

ID: CONSOLE-243

Level: SEVERE

Description: Creation of sub configuration failed.

Data: name of service, name of base global sub configuration, name of sub configuration to be created, name of sub schema to be created, error message

Triggers: Unable to create sub configuration. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.

Actions: Look under service management log for more information.

SMS_EXCEPTION_CREATE_GLOBAL_SUB_CONFIGURATION

ID: CONSOLE-244

Level: SEVERE

Description: Creation of sub configuration failed.

Data: name of service, name of base global sub configuration, name of sub configuration to be created, name of sub schema to be created, error message

Triggers: Unable to create sub configuration due to service management error.

Actions: Look under service management log for more information.

SUCCEED_READ_GLOBAL_SUB_CONFIGURATION_ATTRIBUTE_VALUES

ID: CONSOLE-251

Level: INFO

Description: Reading of sub configuration's attribute values succeeded

Data: name of service, name of sub configuration

Triggers: View sub configuration profile view.

ATTEMPT_WRITE_GLOBAL_SUB_CONFIGURATION_ATTRIBUTE_VALUES

ID: CONSOLE-261

Level: INFO

Description: Attempt to write sub configuration's attribute values

Data: name of service, name of sub configuration

Triggers: Click on save button in sub configuration profile view.

SUCCEED_WRITE_GLOBAL_SUB_CONFIGURATION_ATTRIBUTE_VALUES

ID: CONSOLE-262

Level: INFO

Description: Writing of sub configuration's attribute values succeeded

Data: name of service, name of sub configuration

Triggers: Click on save button in sub configuration profile view.

SSO_EXCEPTION_WRITE_GLOBAL_SUB_CONFIGURATION_ATTRIBUTE_VALUES

ID: CONSOLE-263

Level: SEVERE

Description: Writing of sub configuration's attribute value failed.

Data: name of service, name of sub configuration, error message

Triggers: Unable to write sub configuration's attribute values. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.

Actions: Look under service management log for more information.

SMS_EXCEPTION_WRITE_GLOBAL_SUB_CONFIGURATION_ATTRIBUTE_VALUES_NAMES

ID: CONSOLE-264

Level: SEVERE

Description: Writing of sub configuration's attribute value failed.

Data: name of service, name of sub configuration, error message

Triggers: Unable to write sub configuration's attribute value due to service management error.

Actions: Look under service management log for more information.

ATTEMPT_GET_POLICY_NAMES

ID: CONSOLE-301

Level: INFO

Description: Attempt to get policy names under a realm.

Data: name of realm

Triggers: View policy main page.

SUCCEED_GET_POLICY_NAMES

ID: CONSOLE-302

Level: INFO

Description: Getting policy names under a realm succeeded

Data: name of realm

Triggers: View policy main page.

SSO_EXCEPTION_GET_POLICY_NAMES

ID: CONSOLE-303

Level: SEVERE

Description: Getting policy names under a realm failed.

Data: name of realm, error message

Triggers: Unable to get policy names under a realm. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.

Actions: Look under policy log for more information.

POLICY_EXCEPTION_GET_POLICY_NAMES

ID: CONSOLE-304

Level: SEVERE

Description: Getting policy names under a realm failed.

Data: name of realm, error message

Triggers: Unable to get policy names under a realm due to policy SDK related errors.

Actions: Look under policy log for more information.

ATTEMPT_CREATE_POLICY

ID: CONSOLE-311

Level: INFO

Description: Attempt to create policy under a realm.

Data: name of realm, name of policy

Triggers: Click on New button in policy creation page.

SUCCEED_CREATE_POLICY

ID: CONSOLE-312

Level: INFO

Description: Creation of policy succeeded

Data: name of realm, name of policy

Triggers: Click on New button in policy creation page.

SSO_EXCEPTION_CREATE_POLICY

ID: CONSOLE-313

Level: SEVERE

Description: Creation of policy failed.

Data: name of realm, name of policy, error message

Triggers: Unable to create policy under a realm. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.

Actions: Look under policy log for more information.

POLICY_EXCEPTION_CREATE_POLICY

ID: CONSOLE-314

Level: SEVERE

Description: Creation of policy failed.

Data: name of realm, name of policy, error message

Triggers: Unable to create policy under a realm due to policy SDK related errors.

Actions: Look under policy log for more information.

ATTEMPT_MODIFY_POLICY

ID: CONSOLE-321

Level: INFO

Description: Attempt to modify policy.

Data: name of realm, name of policy

Triggers: Click on Save button in policy profile page.

SUCCEED_MODIFY_POLICY

ID: CONSOLE-322

Level: INFO

Description: Modification of policy succeeded

Data: name of realm, name of policy

Triggers: Click on Save button in policy profile page.

SSO_EXCEPTION_MODIFY_POLICY

ID: CONSOLE-323

Level: SEVERE

Description: Modification of policy failed.

Data: name of realm, name of policy, error message

Triggers: Unable to modify policy under a realm. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.

Actions: Look under policy log for more information.

POLICY_EXCEPTION_MODIFY_POLICY

ID: CONSOLE-324

Level: SEVERE

Description: Modification of policy failed.

Data: name of realm, name of policy, error message

Triggers: Unable to modify policy due to policy SDK related errors.

Actions: Look under policy log for more information.

ATTEMPT_DELETE_POLICY

ID: CONSOLE-331

Level: INFO

Description: Attempt to delete policy.

Data: name of realm, names of policies

Triggers: Click on Delete button in policy main page.

SUCCEED_DELETE_POLICY

ID: CONSOLE-332

Level: INFO

Description: Deletion of policy succeeded

Data: name of realm, name of policies

Triggers: Click on Delete button in policy main page.

SSO_EXCEPTION_DELETE_POLICY

ID: CONSOLE-333

Level: SEVERE

Description: Deletion of policy failed.

Data: name of realm, name of policies, error message

Triggers: Unable to delete policy. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.

Actions: Look under policy log for more information.

POLICY_EXCEPTION_DELETE_POLICY

ID: CONSOLE-334

Level: SEVERE

Description: Deletion of policy failed.

Data: name of realm, name of policies, error message

Triggers: Unable to delete policy due to policy SDK related errors.

Actions: Look under policy log for more information.

ATTEMPT_GET_REALM_NAMES

ID: CONSOLE-401

Level: INFO

Description: Attempt to get realm names

Data: name of parent realm

Triggers: View realm main page.

SUCCEED_GET_REALM_NAMES

ID: CONSOLE-402

Level: INFO

Description: Getting realm names succeeded.

Data: name of parent realm

Triggers: View realm main page.

SMS_EXCEPTION_GET_REALM_NAMES

ID: CONSOLE-403

Level: SEVERE

Description: Getting realm names failed.

Data: name of parent realm, error message

Triggers: Unable to get realm names due to service management SDK exception.

Actions: Look under service management log for more information.

ATTEMPT_CREATE_REALM

ID: CONSOLE-411

Level: INFO

Description: Attempt to create realm

Data: name of parent realm, name of new realm

Triggers: Click on New button in create realm page.

SUCCEED_CREATE_REALM

ID: CONSOLE-412

Level: INFO

Description: Creation of realm succeeded.

Data: name of parent realm, name of new realm

Triggers: Click on New button in create realm page.

SMS_EXCEPTION_CREATE_REALM

ID: CONSOLE-413

Level: SEVERE

Description: Creation of realm failed.

Data: name of parent realm, name of new realm, error message

Triggers: Unable to create new realm due to service management SDK exception.

Actions: Look under service management log for more information.

ATTEMPT_DELETE_REALM

ID: CONSOLE-421

Level: INFO

Description: Attempt to delete realm

Data: name of parent realm, name of realm to delete

Triggers: Click on Delete button in realm main page.

SUCCEED_DELETE_REALM

ID: CONSOLE-422

Level: INFO

Description: Deletion of realm succeeded.

Data: name of parent realm, name of realm to delete

Triggers: Click on Delete button in realm main page.

SMS_EXCEPTION_DELETE_REALM

ID: CONSOLE-423

Level: SEVERE

Description: Deletion of realm failed.

Data: name of parent realm, name of realm to delete, error message

Triggers: Unable to delete realm due to service management SDK exception.

Actions: Look under service management log for more information.

ATTEMPT_GET_ATTR_VALUES_OF_REALM

ID: CONSOLE-431

Level: INFO

Description: Attempt to get attribute values of realm

Data: name of realm

Triggers: View realm profile page.

SUCCEED_GET_ATTR_VALUES_OF_REALM

ID: CONSOLE-432

Level: INFO

Description: Getting attribute values of realm succeeded.

Data: name of realm

Triggers: View realm profile page.

SMS_EXCEPTION_GET_ATTR_VALUES_OF_REALM

ID: CONSOLE-433

Level: SEVERE

Description: Getting attribute values of realm failed.

Data: name of realm, error message

Triggers: Unable to get attribute values of realm due to service management SDK exception.

Actions: Look under service management log for more information.

ATTEMPT_SET_ATTR_VALUES_OF_REALM

ID: CONSOLE-441

Level: INFO

Description: Attempt to modify realm's profile

Data: name of realm

Triggers: Click on Save button in realm profile page.

SUCCEED_SET_ATTR_VALUES_OF_REALM

ID: CONSOLE-442

Level: INFO

Description: Modification of realm's profile succeeded.

Data: name of realm

Triggers: Click on Save button in realm profile page.

SMS_EXCEPTION_SET_ATTR_VALUES_OF_REALM

ID: CONSOLE-443

Level: SEVERE

Description: Modification of realm's profile failed.

Data: name of realm, error message

Triggers: Unable to modify realm's profile due to service management SDK exception.

Actions: Look under service management log for more information.

ATTEMPT_GET_DELEGATION_SUBJECTS

ID: CONSOLE-501

Level: INFO

Description: Attempt to get delegation subjects under a realm

Data: name of realm, search pattern

Triggers: View delegation main page.

SUCCEED_GET_DELEGATION_SUBJECTS

ID: CONSOLE-502

Level: INFO

Description: Getting delegation subjects under a realm succeeded.

Data: name of realm, search pattern

Triggers: View delegation main page.

SSO_EXCEPTION_GET_DELEGATION_SUBJECTS

ID: CONSOLE-503

Level: SEVERE

Description: Getting delegation subjects under a realm failed.

Data: name of realm, search pattern, error message

Triggers: Unable to get delegation subjects. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.

Actions: Look under delegation management log for more information.

DELEGATION_EXCEPTION_GET_DELEGATION_SUBJECTS

ID: CONSOLE-504

Level: SEVERE

Description: Getting delegation subjects under a realm failed.

Data: name of realm, search pattern, error message

Triggers: Unable to get delegation subjects due to delegation management SDK related errors.

Actions: Look under delegation management log for more information.

ATTEMPT_GET_PRIVILEGES_OF_DELEGATION_SUBJECT

ID: CONSOLE-511

Level: INFO

Description: Attempt to get privileges of delegation subject

Data: name of realm, ID of delegation subject

Triggers: View delegation subject profile page.

SUCCEED_GET_PRIVILEGES_OF_DELEGATION_SUBJECT

ID: CONSOLE-512

Level: INFO

Description: Getting privileges of delegation subject succeeded.

Data: name of realm, ID of delegation subject

Triggers: View delegation subject profile page.

SSO_EXCEPTION_GET_PRIVILEGES_OF_DELEGATION_SUBJECT

ID: CONSOLE-513

Level: SEVERE

Description: Getting privileges of delegation subject failed.

Data: name of realm, ID of delegation subject, error message

Triggers: Unable to get privileges of delegation subject. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.

Actions: Look under delegation management log for more information.

DELEGATION_EXCEPTION_GET_PRIVILEGES_OF_DELEGATION_SUBJECT

ID: CONSOLE-514

Level: SEVERE

Description: Getting privileges of delegation subject failed.

Data: name of realm, ID of delegation subject, error message

Triggers: Unable to get privileges of delegation subject due to delegation management SDK related errors.

Actions: Look under delegation management log for more information.

ATTEMPT_MODIFY_DELEGATION_PRIVILEGE

ID: CONSOLE-521

Level: INFO

Description: Attempt to modify delegation privilege

Data: name of realm, ID of delegation privilege, ID of subject

Triggers: Click on Save button in delegation subject profile page.

SUCCEED_MODIFY_DELEGATION_PRIVILEGE

ID: CONSOLE-522

Level: INFO

Description: Modification of delegation privilege succeeded.

Data: name of realm, ID of delegation privilege, ID of subject

Triggers: Click on Save button in delegation subject profile page.

SSO_EXCEPTION_MODIFY_DELEGATION_PRIVILEGE

ID: CONSOLE-523

Level: SEVERE

Description: Modification of delegation privilege failed.

Data: name of realm, ID of delegation privilege, ID of subject, error message

Triggers: Unable to modify delegation privilege. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.

Actions: Look under delegation management log for more information.

DELEGATION_EXCEPTION_MODIFY_DELEGATION_PRIVILEGE

ID: CONSOLE-524

Level: SEVERE

Description: Modification of delegation privilege failed.

Data: name of realm, ID of delegation privilege, ID of subject, error message

Triggers: Unable to modify delegation privilege due to delegation management SDK related errors.

Actions: Look under delegation management log for more information.

ATTEMPT_GET_ID_REPO_NAMES

ID: CONSOLE-601

Level: INFO

Description: Attempt to get data store names

Data: name of realm

Triggers: View data store main page.

SUCCEED_GET_ID_REPO_NAMES

ID: CONSOLE-602

Level: INFO

Description: Getting data store names succeeded.

Data: name of realm

Triggers: View data store main page.

SSO_EXCEPTION_GET_ID_REPO_NAMES

ID: CONSOLE-603

Level: SEVERE

Description: Getting data store names failed.

Data: name of realm, error message

Triggers: Unable to get data store names. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.

Actions: Look under service management log for more information.

SMS_EXCEPTION_GET_ID_REPO_NAMES

ID: CONSOLE-604

Level: SEVERE

Description: Getting data store names failed.

Data: name of realm, error message

Triggers: Unable to get data store names due to service management SDK exception.

Actions: Look under service management log for more information.

ATTEMPT_GET_ATTR_VALUES_ID_REPO

ID: CONSOLE-611

Level: INFO

Description: Attempt to get attribute values of identity repository

Data: name of realm, name of identity repository

Triggers: View data store profile page.

SUCCEED_GET_ATTR_VALUES_ID_REPO

ID: CONSOLE-612

Level: INFO

Description: Getting attribute values of data store succeeded.

Data: name of realm, name of identity repository

Triggers: View data store profile page.

SSO_EXCEPTION_GET_ATTR_VALUES_ID_REPO

ID: CONSOLE-613

Level: SEVERE

Description: Getting attribute values of data store failed.

Data: name of realm, name of identity repository, error message

Triggers: Unable to get attribute values of identity repository. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.

Actions: Look under service management log for more information.

SMS_EXCEPTION_GET_ATTR_VALUES_ID_REPO

ID: CONSOLE-614

Level: SEVERE

Description: Getting attribute values of data store failed.

Data: name of realm, name of identity repository, error message

Triggers: Unable to get attribute values of data store due to service management SDK exception.

Actions: Look under service management log for more information.

ATTEMPT_CREATE_ID_REPO

ID: CONSOLE-621

Level: INFO

Description: Attempt to create identity repository

Data: name of realm, name of identity repository, type of identity repository

Triggers: Click on New button in data store creation page.

SUCCEED_CREATE_ID_REPO

ID: CONSOLE-622

Level: INFO

Description: Creation of data store succeeded.

Data: name of realm, name of identity repository, type of identity repository

Triggers: Click on New button in data store creation page.

SSO_EXCEPTION_CREATE_ID_REPO

ID: CONSOLE-623

Level: SEVERE

Description: Creation of data store failed.

Data: name of realm, name of identity repository, type of identity repository, error message

Triggers: Unable to create identity repository. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.

Actions: Look under service management log for more information.

SMS_EXCEPTION_CREATE_ID_REPO

ID: CONSOLE-624

Level: SEVERE

Description: Creation data store failed.

Data: name of realm, name of identity repository, type of identity repository, error message

Triggers: Unable to create data store due to service management SDK exception.

Actions: Look under service management log for more information.

ATTEMPT_DELETE_ID_REPO

ID: CONSOLE-631

Level: INFO

Description: Attempt to delete identity repository

Data: name of realm, name of identity repository

Triggers: Click on Delete button in data store main page.

SUCCEED_DELETE_ID_REPO

ID: CONSOLE-632

Level: INFO

Description: Deletion of data store succeeded.

Data: name of realm, name of identity repository

Triggers: Click on Delete button in data store main page.

SSO_EXCEPTION_DELETE_ID_REPO

ID: CONSOLE-633

Level: SEVERE

Description: Deletion of data store failed.

Data: name of realm, name of identity repository, error message

Triggers: Unable to delete identity repository. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.

Actions: Look under service management log for more information.

SMS_EXCEPTION_DELETE_ID_REPO

ID: CONSOLE-634

Level: SEVERE

Description: Deletion data store failed.

Data: name of realm, name of identity repository, error message

Triggers: Unable to delete data store due to service management SDK exception.

Actions: Look under service management log for more information.

ATTEMPT_MODIFY_ID_REPO

ID: CONSOLE-641

Level: INFO

Description: Attempt to modify identity repository

Data: name of realm, name of identity repository

Triggers: Click on Save button in data store profile page.

SUCCEED_MODIFY_ID_REPO

ID: CONSOLE-642

Level: INFO

Description: Modification of data store succeeded.

Data: name of realm, name of identity repository

Triggers: Click on Save button in data store profile page.

SSO_EXCEPTION_MODIFY_ID_REPO

ID: CONSOLE-643

Level: SEVERE

Description: Modification of data store failed.

Data: name of realm, name of identity repository, error message

Triggers: Unable to modify identity repository. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.

Actions: Look under service management log for more information.

SMS_EXCEPTION_MODIFY_ID_REPO

ID: CONSOLE-644

Level: SEVERE

Description: Modification data store failed.

Data: name of realm, name of identity repository, error message

Triggers: Unable to modify data store due to service management SDK exception.

Actions: Look under service management log for more information.

ATTEMPT_GET_ASSIGNED_SERVICE_OF_REALM

ID: CONSOLE-701

Level: INFO

Description: Attempt to get assigned services of realm

Data: name of realm

Triggers: View realm's service main page.

SUCCEED_GET_ASSIGNED_SERVICE_OF_REALM

ID: CONSOLE-702

Level: INFO

Description: Getting assigned services of realm succeeded.

Data: name of realm

Triggers: View realm's service main page.

CONFIGURATION_EXCEPTION_GET_ASSIGNED_SERVICE_OF_REALM

ID: CONSOLE-703

Level: SEVERE

Description: Getting assigned services of realm failed.

Data: name of realm, error message

Triggers: Unable to get assigned services of realm due authentication configuration exception.

Actions: Look under authentication log for more information.

SMS_EXCEPTION_GET_ASSIGNED_SERVICE_OF_REALM

ID: CONSOLE-704

Level: SEVERE

Description: Getting assigned services of realm failed.

Data: name of realm, error message

Triggers: Unable to get assigned services of realm due to service management SDK exception.

Actions: Look under service management log for more information.

IDREPO_EXCEPTION_GET_ASSIGNED_SERVICE_OF_REALM

ID: CONSOLE-705

Level: SEVERE

Description: Getting assigned services of realm failed.

Data: name of realm, error message

Triggers: Unable to get assigned services of realm due to data store SDK exception.

Actions: Look under service management log for more information.

SSO_EXCEPTION_GET_ASSIGNED_SERVICE_OF_REALM

ID: CONSOLE-706

Level: SEVERE

Description: Getting assigned services of realm failed.

Data: name of realm, error message

Triggers: Unable to get assigned services of realm. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.

Actions: Look under service management log for more information.

ATTEMPT_GET_ASSIGNABLE_SERVICE_OF_REALM

ID: CONSOLE-711

Level: INFO

Description: Attempt to get assignable services of realm

Data: name of realm

Triggers: View realm's service main page.

SUCCEED_GET_ASSIGNABLE_SERVICE_OF_REALM

ID: CONSOLE-712

Level: INFO

Description: Getting assignable services of realm succeeded.

Data: name of realm

Triggers: View realm's service main page.

CONFIGURATION_EXCEPTION_GET_ASSIGNABLE_SERVICE_OF_REALM

ID: CONSOLE-713

Level: SEVERE

Description: Getting assignable services of realm failed.

Data: name of realm, error message

Triggers: Unable to get assignable services of realm due authentication configuration exception.

Actions: Look under authentication log for more information.

SMS_EXCEPTION_GET_ASSIGNABLE_SERVICE_OF_REALM

ID: CONSOLE-714

Level: SEVERE

Description: Getting assignable services of realm failed.

Data: name of realm, error message

Triggers: Unable to get assignable services of realm due to service management SDK exception.

Actions: Look under service management log for more information.

IDREPO_EXCEPTION_GET_ASSIGNABLE_SERVICE_OF_REALM

ID: CONSOLE-715

Level: SEVERE

Description: Getting assignable services of realm failed.

Data: name of realm, error message

Triggers: Unable to get assignable services of realm due to ID Repository management SDK exception.

Actions: Look under ID Repository management log for more information.

SSO_EXCEPTION_GET_ASSIGNABLE_SERVICE_OF_REALM

ID: CONSOLE-716

Level: SEVERE

Description: Getting assignable services of realm failed.

Data: name of realm, error message

Triggers: Unable to get assignable services of realm. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.

Actions: Look under service management log for more information.

ATTEMPT_UNASSIGN_SERVICE_FROM_REALM

ID: CONSOLE-721

Level: INFO

Description: Attempt to unassign service from realm

Data: name of realm, name of service

Triggers: Click on Unassign button in realm's service page.

SUCCEED_UNASSIGN_SERVICE_FROM_REALM

ID: CONSOLE-722

Level: INFO

Description: Unassign service from realm succeeded.

Data: name of realm, name of service

Triggers: Click on Unassign button in realm's service page.

SMS_EXCEPTION_UNASSIGN_SERVICE_FROM_REALM

ID: CONSOLE-723

Level: SEVERE

Description: Unassign service from realm failed.

Data: name of realm, name of service, error message

Triggers: Unable to unassign service from realm due to service management SDK exception.

Actions: Look under service management log for more information.

SSO_EXCEPTION_UNASSIGN_SERVICE_FROM_REALM

ID: CONSOLE-725

Level: SEVERE

Description: Unassign service from realm failed.

Data: name of realm, name of service, error message

Triggers: Unable to unassign service from realm. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.

Actions: Look under data store management log for more information.

IDREPO_EXCEPTION_UNASSIGN_SERVICE_FROM_REALM

ID: CONSOLE-724

Level: SEVERE

Description: Unassign service from realm failed.

Data: name of realm, name of service, error message

Triggers: Unable to unassign service from realm due to data store management SDK exception.

Actions: Look under data store management log for more information.

ATTEMPT_ASSIGN_SERVICE_TO_REALM

ID: CONSOLE-731

Level: INFO

Description: Attempt to assign service to realm

Data: name of realm, name of service

Triggers: Click on assign button in realm's service page.

SUCCEED_ASSIGN_SERVICE_TO_REALM

ID: CONSOLE-732

Level: INFO

Description: Assignment of service to realm succeeded.

Data: name of realm, name of service

Triggers: Click on assign button in realm's service page.

SMS_EXCEPTION_ASSIGN_SERVICE_TO_REALM

ID: CONSOLE-733

Level: SEVERE

Description: Assignment of service to realm failed.

Data: name of realm, name of service, error message

Triggers: Unable to assign service to realm due to service management SDK exception.

Actions: Look under service management log for more information.

SSO_EXCEPTION_ASSIGN_SERVICE_TO_REALM

ID: CONSOLE-734

Level: SEVERE

Description: Assignment of service to realm failed.

Data: name of realm, name of service, error message

Triggers: Unable to assign service to realm. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.

Actions: Look under service management log for more information.

IDREPO_EXCEPTION_ASSIGN_SERVICE_TO_REALM

ID: CONSOLE-735

Level: SEVERE

Description: Assignment of service to realm failed.

Data: name of realm, name of service, error message

Triggers: Unable to assign service to realm due to data store SDK exception.

Actions: Look under service management log for more information.

ATTEMPT_GET_ATTR_VALUE_OF_SERVICE_UNDER_REALM

ID: CONSOLE-741

Level: INFO

Description: Attempt to get attribute values of service in realm

Data: name of realm, name of service, name of attribute schema

Triggers: View realm's service profile page.

SUCCEED_GET_ATTR_VALUE_OF_SERVICE_UNDER_REALM

ID: CONSOLE-742

Level: INFO

Description: Getting of attribute values of service under realm succeeded.

Data: name of realm, name of service, name of attribute schema

Triggers: View realm's service profile page.

SMS_EXCEPTION_GET_ATTR_VALUE_OF_SERVICE_UNDER_REALM

ID: CONSOLE-743

Level: SEVERE

Description: Getting of attribute values of service under realm failed.

Data: name of realm, name of service, name of attribute schema, error message

Triggers: Unable to get attribute values of service due to service management SDK exception.

Actions: Look under service management log for more information.

IDREPO_EXCEPTION_GET_ATTR_VALUE_OF_SERVICE_UNDER_REALM

ID: CONSOLE-744

Level: INFO

Description: Getting of attribute values of service under realm failed.

Data: name of realm, name of service, name of attribute schema, error message

Triggers: Unable to get attribute values of service due to data store SDK exception.

Actions: Look under service management log for more information.

SSO_EXCEPTION_GET_ATTR_VALUE_OF_SERVICE_UNDER_REALM

ID: CONSOLE-745

Level: SEVERE

Description: Getting of attribute values of service under realm failed.

Data: name of realm, name of service, name of attribute schema, error message

Triggers: Unable to get attribute values of service. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.

Actions: Look under service management log for more information.

ATTEMPT_MODIFY_SERVICE_UNDER_REALM

ID: CONSOLE-751

Level: INFO

Description: Attempt to modify attribute values of service in realm

Data: name of realm, name of service

Triggers: Click on Save button in realm's service profile page.

SUCCEED_MODIFY_SERVICE_UNDER_REALM

ID: CONSOLE-752

Level: INFO

Description: Modification of attribute values of service under realm succeeded.

Data: name of realm, name of service

Triggers: Click on Save button in realm's service profile page.

SMS_EXCEPTION_MODIFY_SERVICE_UNDER_REALM

ID: CONSOLE-753

Level: SEVERE

Description: Modification of attribute values of service under realm failed.

Data: name of realm, name of service, error message

Triggers: Unable to modify attribute values of service due to service management SDK exception.

Actions: Look under service management log for more information.

IDREPO_EXCEPTION_MODIFY_SERVICE_UNDER_REALM

ID: CONSOLE-754

Level: SEVERE

Description: Modification of attribute values of service under realm failed.

Data: name of realm, name of service, error message

Triggers: Unable to modify attribute values of service due to data store error.

Actions: Look under data store log for more information.

SSO_EXCEPTION_MODIFY_SERVICE_UNDER_REALM

ID: CONSOLE-755

Level: SEVERE

Description: Modification of attribute values of service under realm failed.

Data: name of realm, name of service, error message

Triggers: Unable to modify attribute values of service. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation

Actions: Look under data store log for more information.

ATTEMPT_GET_AUTH_TYPE

ID: CONSOLE-801

Level: INFO

Description: Attempt to get authentication type

Data: server instance name

Triggers: View authentication profile page.

SUCCEED_GET_AUTH_TYPE

ID: CONSOLE-802

Level: INFO

Description: Getting of authentication type succeeded.

Data: server instance name

Triggers: View authentication profile page.

SMS_EXCEPTION_GET_AUTH_TYPE

ID: CONSOLE-803

Level: SEVERE

Description: Getting of authentication type failed.

Data: error message

Triggers: Unable to get authentication type due to authentication configuration SDK exception.

Actions: Look under authentication management log for more information.

ATTEMPT_GET_AUTH_INSTANCE

ID: CONSOLE-811

Level: INFO

Description: Attempt to get authentication instances under a realm

Data: name of realm

Triggers: View authentication profile page.

SUCCEED_GET_AUTH_INSTANCE

ID: CONSOLE-812

Level: INFO

Description: Getting of authentication instances under a realm succeeded.

Data: name of realm

Triggers: View authentication profile page.

AUTH_CONFIG_EXCEPTION_GET_AUTH_INSTANCE

ID: CONSOLE-813

Level: SEVERE

Description: Getting of authentication instances under a realm failed.

Data: name of realm, error message

Triggers: Unable to get authentication instance due to authentication configuration SDK exception.

Actions: Look under authentication management log for more information.

ATTEMPT_REMOVE_AUTH_INSTANCE

ID: CONSOLE-821

Level: INFO

Description: Attempt to remove authentication instances under a realm

Data: name of realm, name of authentication instance

Triggers: View authentication profile page.

SUCCEED_REMOVE_AUTH_INSTANCE

ID: CONSOLE-822

Level: INFO

Description: Removal of authentication instances under a realm succeeded.

Data: name of realm, name of authentication instance

Triggers: View authentication profile page.

AUTH_CONFIG_EXCEPTION_REMOVE_AUTH_INSTANCE

ID: CONSOLE-823

Level: SEVERE

Description: Removal of authentication instances under a realm failed.

Data: name of realm, name of authentication instance, error message

Triggers: Unable to remove authentication instance due to authentication configuration SDK exception.

Actions: Look under authentication management log for more information.

ATTEMPT_CREATE_AUTH_INSTANCE

ID: CONSOLE-831

Level: INFO

Description: Attempt to create authentication instance under a realm

Data: name of realm, name of authentication instance, type of authentication instance

Triggers: Click on New button in authentication creation page.

SUCCEED_CREATE_AUTH_INSTANCE

ID: CONSOLE-832

Level: INFO

Description: Creation of authentication instance under a realm succeeded.

Data: name of realm, name of authentication instance, type of authentication instance

Triggers: Click on New button in authentication creation page.

AUTH_CONFIG_EXCEPTION_CREATE_AUTH_INSTANCE

ID: CONSOLE-833

Level: SEVERE

Description: Creation of authentication instance under a realm failed.

Data: name of realm, name of authentication instance, type of authentication instance, error message

Triggers: Unable to create authentication instance due to authentication configuration exception.

Actions: Look under authentication configuration log for more information.

ATTEMPT_MODIFY_AUTH_INSTANCE

ID: CONSOLE-841

Level: INFO

Description: Attempt to modify authentication instance

Data: name of realm, name of authentication service

Triggers: Click on Save button in authentication profile page.

SUCCEED_MODIFY_AUTH_INSTANCE

ID: CONSOLE-842

Level: INFO

Description: Modification of authentication instance succeeded.

Data: name of realm, name of authentication service

Triggers: Click on Save button in authentication profile page.

SMS_EXCEPTION_MODIFY_AUTH_INSTANCE

ID: CONSOLE-843

Level: SEVERE

Description: Modification of authentication instance failed.

Data: name of realm, name of authentication service, error message

Triggers: Unable to modify authentication instance due to service management SDK exception.

Actions: Look under service anagement log for more information.

SSO_EXCEPTION_MODIFY_AUTH_INSTANCE

ID: CONSOLE-844

Level: SEVERE

Description: Modification of authentication instance failed.

Data: name of realm, name of authentication service, error message

Triggers: Unable to modify authentication instance. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.

Actions: Look under service management log for more information.

ATTEMPT_GET_AUTH_INSTANCE_PROFILE

ID: CONSOLE-851

Level: INFO

Description: Attempt to get authentication instance profile

Data: name of realm, name of authentication instance

Triggers: View authentication instance profile page.

SUCCEED_GET_AUTH_INSTANCE_PROFILE

ID: CONSOLE-852

Level: INFO

Description: Getting of authentication instance profile succeeded.

Data: name of realm, name of authentication instance

Triggers: View authentication instance profile page.

AUTH_CONFIGURATION_EXCEPTION_GET_AUTH_INSTANCE_PROFILE

ID: CONSOLE-853

Level: SEVERE

Description: Getting of authentication instance profile failed.

Data: name of realm, name of authentication instance, error message

Triggers: Unable to get authentication instance profile due to authentication configuration SDK exception.

Actions: Look under authentication management log for more information.

ATTEMPT_MODIFY_AUTH_INSTANCE_PROFILE

ID: CONSOLE-861

Level: INFO

Description: Attempt to modify authentication instance profile

Data: name of realm, name of authentication instance

Triggers: Click on Save button in authentication instance profile page.

SUCCEED_MODIFY_AUTH_INSTANCE_PROFILE

ID: CONSOLE-862

Level: INFO

Description: Modification of authentication instance profile succeeded.

Data: name of realm, name of authentication instance

Triggers: Click on Save button in authentication instance profile page.

AUTH_CONFIGURATION_EXCEPTION_MODIFY_AUTH_INSTANCE_PROFILE

ID: CONSOLE-863

Level: SEVERE

Description: Modification of authentication instance profile failed.

Data: name of realm, name of authentication instance, error message

Triggers: Unable to modify authentication instance profile due to authentication configuration SDK exception.

Actions: Look under authentication management log for more information.

SMS_EXCEPTION_MODIFY_AUTH_INSTANCE_PROFILE

ID: CONSOLE-864

Level: SEVERE

Description: Modification of authentication instance profile failed.

Data: name of realm, name of authentication instance, error message

Triggers: Unable to modify authentication instance profile due to service management SDK exception.

Actions: Look under service management log for more information.

SSO_EXCEPTION_MODIFY_AUTH_INSTANCE_PROFILE

ID: CONSOLE-865

Level: SEVERE

Description: Modification of authentication instance profile failed.

Data: name of realm, name of authentication instance, error message

Triggers: Unable to modify authentication instance profile. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.

Actions: Look under service management log for more information.

ATTEMPT_GET_AUTH_PROFILE_IN_REALM

ID: CONSOLE-871

Level: INFO

Description: Attempt to get authentication profile under a realm

Data: name of realm

Triggers: View authentication profile under a realm page.

SUCCEED_GET_AUTH_PROFILE_IN_REALM

ID: CONSOLE-872

Level: INFO

Description: Getting authentication profile under a realm succeeded.

Data: name of realm

Triggers: View authentication profile under a realm page.

SMS_CONFIGURATION_EXCEPTION_GET_AUTH_PROFILE_IN_REALM

ID: CONSOLE-873

Level: SEVERE

Description: Getting authentication profile under a realm failed.

Data: name of realm, error message

Triggers: Unable to get authentication profile under a realm due to service management SDK exception.

Actions: Look under service management log for more information.

ATTEMPT_GET_AUTH_CONFIG_PROFILE

ID: CONSOLE-881

Level: INFO

Description: Attempt to get authentication configuration profile

Data: name of realm, name of authentication configuration

Triggers: View authentication configuration profile page.

SUCCEED_GET_AUTH_CONFIG_PROFILE

ID: CONSOLE-882

Level: INFO

Description: Getting authentication configuration profile succeeded.

Data: name of realm, name of authentication configuration

Triggers: View authentication configuration profile page.

SSO_EXCEPTION_GET_AUTH_CONFIG_PROFILE

ID: CONSOLE-883

Level: SEVERE

Description: Getting authentication configuration profile failed.

Data: name of realm, name of authentication configuration, error message

Triggers: Unable to get authentication configuration profile. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.

Actions: Look under service management log for more information.

SMS_EXCEPTION_GET_AUTH_CONFIG_PROFILE

ID: CONSOLE-884

Level: SEVERE

Description: Getting authentication configuration profile failed.

Data: name of realm, name of authentication configuration, error message

Triggers: Unable to get authentication configuration profile due to service management SDK exception.

Actions: Look under service management log for more information.

AUTH_CONFIGURATION_EXCEPTION_GET_AUTH_CONFIG_PROFILE

ID: CONSOLE-885

Level: SEVERE

Description: Getting authentication configuration profile failed.

Data: name of realm, name of authentication configuration, error message

Triggers: Unable to get authentication configuration profile due to authentication configuration SDK exception.

Actions: Look under authentication configuration log for more information.

ATTEMPT_MODIFY_AUTH_CONFIG_PROFILE

ID: CONSOLE-891

Level: INFO

Description: Attempt to modify authentication configuration profile

Data: name of realm, name of authentication configuration

Triggers: Click on Save button in authentication configuration profile page.

SUCCEED_MODIFY_AUTH_CONFIG_PROFILE

ID: CONSOLE-892

Level: INFO

Description: Modification of authentication configuration profile succeeded.

Data: name of realm, name of authentication configuration

Triggers: Click on Save button in authentication configuration profile page.

SSO_EXCEPTION_MODIFY_AUTH_CONFIG_PROFILE

ID: CONSOLE-893

Level: SEVERE

Description: Modification of authentication configuration profile failed.

Data: name of realm, name of authentication configuration, error message

Triggers: Unable to modify authentication configuration profile. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.

Actions: Look under service management log for more information.

SMS_EXCEPTION_MODIFY_AUTH_CONFIG_PROFILE

ID: CONSOLE-894

Level: SEVERE

Description: Modification of authentication configuration profile failed.

Data: name of realm, name of authentication configuration, error message

Triggers: Unable to modify authentication configuration profile due to service management SDK exception.

Actions: Look under service management log for more information.

AUTH_CONFIGURATION_EXCEPTION_MODIFY_AUTH_CONFIG_PROFILE

ID: CONSOLE-895

Level: SEVERE

Description: Modification of authentication configuration profile failed.

Data: name of realm, name of authentication configuration, error message

Triggers: Unable to modify authentication configuration profile due to authentication configuration SDK exception.

Actions: Look under authentication configuration log for more information.

ATTEMPT_CREATE_AUTH_CONFIG

ID: CONSOLE-901

Level: INFO

Description: Attempt to create authentication configuration

Data: name of realm, name of authentication configuration

Triggers: Click on New button in authentication configuration creation page.

SUCCEED_CREATE_AUTH_CONFIG

ID: CONSOLE-902

Level: INFO

Description: Creation of authentication configuration succeeded.

Data: name of realm, name of authentication configuration

Triggers: Click on New button in authentication configuration creation page.

SSO_EXCEPTION_CREATE_AUTH_CONFIG

ID: CONSOLE-903

Level: SEVERE

Description: Creation of authentication configuration failed.

Data: name of realm, name of authentication configuration, error message

Triggers: Unable to create authentication configuration. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.

Actions: Look under service management log for more information.

SMS_EXCEPTION_CREATE_AUTH_CONFIG

ID: CONSOLE-904

Level: SEVERE

Description: Creation of authentication configuration failed.

Data: name of realm, name of authentication configuration, error message

Triggers: Unable to create authentication configuration due to service management SDK exception.

Actions: Look under service management log for more information.

AUTH_CONFIGURATION_EXCEPTION_CREATE_AUTH_CONFIG

ID: CONSOLE-905

Level: SEVERE

Description: Creation of authentication configuration failed.

Data: name of realm, name of authentication configuration, error message

Triggers: Unable to create authentication configuration due to authentication configuration SDK exception.

Actions: Look under authentication configuration log for more information.

ATTEMPT_GET_ENTITY_DESCRIPTOR

ID: CONSOLE-1001

Level: INFO

Description: Attempt to get entity descriptor names.

Data: search pattern

Triggers: View entity descriptor main page.

SUCCEED_GET_ENTITY_DESCRIPTOR

ID: CONSOLE-1002

Level: INFO

Description: Getting entity descriptor names succeeded

Data: search pattern

Triggers: View entity descriptor main page.

FEDERATION_EXCEPTION_GET_ENTITY_DESCRIPTOR

ID: CONSOLE-1003

Level: SEVERE

Description: Getting entity descriptor names failed.

Data: search pattern, error message

Triggers: Unable to get entity descriptor names due to federation SDK related errors.

Actions: Look under federation log for more information.

ATTEMPT_CREATE_ENTITY_DESCRIPTOR

ID: CONSOLE-1011

Level: INFO

Description: Attempt to create entity descriptor.

Data: descriptor realm, descriptor name, descriptor protocol, descriptor type

Triggers: Click on New button in entity descriptor creation page.

SUCCEED_CREATE_ENTITY_DESCRIPTOR

ID: CONSOLE-1012

Level: INFO

Description: Creation entity descriptor succeeded

Data: descriptor realm, descriptor name, descriptor protocol, descriptor type

Triggers: Click on New button in entity descriptor creation page.

FEDERATION_EXCEPTION_CREATE_ENTITY_DESCRIPTOR

ID: CONSOLE-1013

Level: SEVERE

Description: Creation entity descriptor failed.

Data: descriptor realm, descriptor name, descriptor protocol, descriptor type, error message

Triggers: Unable to create entity descriptor due to federation SDK related errors.

Actions: Look under federation log for more information.

ATTEMPT_DELETE_ENTITY_DESCRIPTORS

ID: CONSOLE-1021

Level: INFO

Description: Attempt to delete entity descriptors.

Data: descriptor names

Triggers: Click on Delete button in entity descriptor main page.

SUCCEED_DELETE_ENTITY_DESCRIPTORS

ID: CONSOLE-1022

Level: INFO

Description: Deletion entity descriptors succeeded

Data: descriptor names

Triggers: Click on Delete button in entity descriptor main page.

FEDERATION_EXCEPTION_DELETE_ENTITY_DESCRIPTORS

ID: CONSOLE-1023

Level: SEVERE

Description: Deletion entity descriptors failed.

Data: descriptor names, error message

Triggers: Unable to delete entity descriptors due to federation SDK related errors.

Actions: Look under federation log for more information.

ATTEMPT_GET_AFFILIATE_ENTITY_DESCRIPTOR_ATTR_VALUES

ID: CONSOLE-1031

Level: INFO

Description: Attempt to get attribute values of an affiliate entity descriptor.

Data: descriptor realm, descriptor name, descriptor protocol

Triggers: View affiliate entity descriptor profile page.

SUCCEED_GET_AFFILIATE_ENTITY_DESCRIPTOR_ATTR_VALUES

ID: CONSOLE-1032

Level: INFO

Description: Getting of attribute values of an affiliate entity descriptor succeeded.

Data: descriptor realm, descriptor name, descriptor protocol

Triggers: View affiliate entity descriptor profile page.

FEDERATION_EXCEPTION_GET_AFFILIATE_ENTITY_DESCRIPTOR_ATTR_VALUES

ID: CONSOLE-1033

Level: SEVERE

Description: Getting of attribute values of an affiliate entity descriptor failed.

Data: descriptor realm, descriptor name, descriptor protocol, error message

Triggers: Unable to get attribute value of an affiliate entity descriptor due to federation SDK related errors.

Actions: Look under federation log for more information.

ATTEMPT_MODIFY_AFFILIATE_ENTITY_DESCRIPTOR

ID: CONSOLE-1041

Level: INFO

Description: Attempt to modify an affiliate entity descriptor.

Data: descriptor realm, descriptor name, descriptor protocol

Triggers: Click on Save button of affiliate entity descriptor profile page.

SUCCEED_MODIFY_AFFILIATE_ENTITY_DESCRIPTOR

ID: CONSOLE-1042

Level: INFO

Description: Modification of an affiliate entity descriptor succeeded.

Data: descriptor realm, descriptor name, descriptor protocol

Triggers: Click on Save button of affiliate entity descriptor profile page.

FEDERATION_EXCEPTION_MODIFY_AFFILIATE_ENTITY_DESCRIPTOR

ID: CONSOLE-1043

Level: SEVERE

Description: Modification of an affiliate entity descriptor failed.

Data: descriptor realm, descriptor name, descriptor protocol, error message

Triggers: Unable to modify an affiliate entity descriptor due to federation SDK related errors.

Actions: Look under federation log for more information.

ATTRIBUTE_FORMAT_EXCEPTION_MODIFY_AFFILIATE_ENTITY_DESCRIPTOR

ID: CONSOLE-1044

Level: SEVERE

Description: Modification of an affiliate entity descriptor failed.

Data: descriptor name, error message

Triggers: Unable to modify an affiliate entity descriptor due to incorrect number format of one or more attribute values.

Actions: Look under federation log for more information.

ATTEMPT_GET_ENTITY_DESCRIPTOR_ATTR_VALUES

ID: CONSOLE-1051

Level: INFO

Description: Attempt to get attribute values of an entity descriptor.

Data: descriptor realm, descriptor name, descriptor protocol, descriptor type

Triggers: View entity descriptor profile page.

SUCCEED_GET_ENTITY_DESCRIPTOR_ATTR_VALUES

ID: CONSOLE-1052

Level: INFO

Description: Getting attribute values of entity descriptor succeeded.

Data: descriptor realm, descriptor name, descriptor protocol, descriptor type

Triggers: View entity descriptor profile page.

FEDERATION_EXCEPTION_GET_ENTITY_DESCRIPTOR_ATTR_VALUES

ID: CONSOLE-1053

Level: SEVERE

Description: Getting attribute values of entity descriptor failed.

Data: descriptor realm, descriptor name, descriptor protocol, descriptor type, error message

Triggers: Unable to get attribute values of entity descriptor due to federation SDK related errors.

Actions: Look under federation log for more information.

ATTEMPT_MODIFY_ENTITY_DESCRIPTOR

ID: CONSOLE-1061

Level: INFO

Description: Attempt to modify entity descriptor.

Data: descriptor realm, descriptor name, descriptor protocol, descriptor type

Triggers: Click on Save button in entity descriptor profile page.

SUCCEED_MODIFY_ENTITY_DESCRIPTOR

ID: CONSOLE-1062

Level: INFO

Description: Modification of entity descriptor succeeded.

Data: descriptor realm, descriptor name, descriptor protocol, descriptor type

Triggers: Click on Save button in entity descriptor profile page.

FEDERATION_EXCEPTION_MODIFY_ENTITY_DESCRIPTOR

ID: CONSOLE-1063

Level: SEVERE

Description: Modification of entity descriptor failed.

Data: descriptor realm, descriptor name, descriptor protocol, descriptor type, error message

Triggers: Unable to modify entity descriptor due to federation SDK related errors.

Actions: Look under federation log for more information.

ATTEMPT_GET_AUTH_DOMAINS

ID: CONSOLE-1101

Level: INFO

Description: Attempt to get authentication domain names.

Data: search pattern

Triggers: View authentication domain main page.

SUCCEED_GET_AUTH_DOMAINS

ID: CONSOLE-1102

Level: INFO

Description: Getting authentication domain names succeeded.

Data: search pattern

Triggers: View authentication domain main page.

FEDERATION_EXCEPTION_GET_AUTH_DOMAINS

ID: CONSOLE-1103

Level: SEVERE

Description: Getting authentication domain names failed.

Data: name of realm, error message

Triggers: Unable to get authentication domain names due to federation SDK related errors.

Actions: Look under federation log for more information.

ATTEMPT_CREATE_AUTH_DOMAIN

ID: CONSOLE-1111

Level: INFO

Description: Attempt to create authentication domain

Data: name of authentication domain

Triggers: Click on New button in authentication domain creation page.

SUCCEED_CREATE_AUTH_DOMAIN

ID: CONSOLE-1112

Level: INFO

Description: Creation authentication domain succeeded.

Data: name of authentication domain

Triggers: Click on New button in authentication domain creation page.

FEDERATION_EXCEPTION_CREATE_AUTH_DOMAIN

ID: CONSOLE-1113

Level: SEVERE

Description: Creation authentication domain failed.

Data: name of authentication domain, error message

Triggers: Unable to create authentication domain due to federation SDK related errors.

Actions: Look under federation log for more information.

ATTEMPT_DELETE_AUTH_DOMAINS

ID: CONSOLE-1121

Level: INFO

Description: Attempt to delete authentication domains

Data: name of realm, name of authentication domains

Triggers: Click on Delete button in authentication domain main page.

SUCCEED_DELETE_AUTH_DOMAIN

ID: CONSOLE-1122

Level: INFO

Description: Deletion authentication domain succeeded.

Data: name of realm, name of authentication domains

Triggers: Click on Delete button in authentication domain main page.

FEDERATION_EXCEPTION_DELETE_AUTH_DOMAIN

ID: CONSOLE-1123

Level: SEVERE

Description: Deletion authentication domain failed.

Data: name of realm, name of authentication domains, error message

Triggers: Unable to delete authentication domain due to federation SDK related errors.

Actions: Look under federation log for more information.

ATTEMPT_GET_AUTH_DOMAIN_ATTR_VALUES

ID: CONSOLE-1131

Level: INFO

Description: Attempt to get authentication domain's attribute values

Data: name of realm, name of authentication domain

Triggers: View authentication domain profile page.

SUCCEED_GET_AUTH_DOMAIN_ATTR_VALUES

ID: CONSOLE-1132

Level: INFO

Description: Getting attribute values of authentication domain succeeded.

Data: name of realm, name of authentication domain

Triggers: View authentication domain profile page.

FEDERATION_EXCEPTION_GET_AUTH_DOMAIN_ATTR_VALUES

ID: CONSOLE-1133

Level: SEVERE

Description: Getting attribute values of authentication domain failed.

Data: name of realm, name of authentication domains, error message

Triggers: Unable to get attribute values of authentication domain due to federation SDK related errors.

Actions: Look under federation log for more information.

ATTEMPT_MODIFY_AUTH_DOMAIN

ID: CONSOLE-1141

Level: INFO

Description: Attempt to modify authentication domain

Data: name of realm, name of authentication domain

Triggers: Click on Save button in authentication domain profile page.

SUCCEED_MODIFY_AUTH_DOMAIN

ID: CONSOLE-1142

Level: INFO

Description: Modification authentication domain succeeded.

Data: name of realm, name of authentication domain

Triggers: Click on Save button in authentication domain profile page.

FEDERATION_EXCEPTION_MODIFY_AUTH_DOMAIN

ID: CONSOLE-1143

Level: SEVERE

Description: Modification authentication domain failed.

Data: name of realm, name of authentication domain, error message

Triggers: Unable to modify authentication domain due to federation SDK related errors.

Actions: Look under federation log for more information.

ATTEMPT_GET_ALL_PROVIDER_NAMES

ID: CONSOLE-1151

Level: INFO

Description: Attempt to get all provider names

Data: realm name

Triggers: View authentication domain profile page.

SUCCEED_GET_ALL_PROVIDER_NAMES

ID: CONSOLE-1152

Level: INFO

Description: Getting all provider names succeeded.

Data: realm name

Triggers: View authentication domain profile page.

FEDERATION_EXCEPTION_GET_ALL_PROVIDER_NAMES

ID: CONSOLE-1153

Level: SEVERE

Description: Getting all provider names failed.

Data: error message

Triggers: Unable to get all provider names due to federation SDK related errors.

Actions: Look under federation log for more information.

ATTEMPT_GET_PROVIDER_NAMES_UNDER_AUTH_DOMAIN

ID: CONSOLE-1161

Level: INFO

Description: Attempt to get provider names under a authentication domain

Data: name of realm, name of authentication domain

Triggers: View authentication domain profile page.

SUCCEED_GET_PROVIDER_NAMES_UNDER_AUTH_DOMAIN

ID: CONSOLE-1162

Level: INFO

Description: Getting provider names under authentication domain succeeded.

Data: name of realm, name of authentication domain

Triggers: View authentication domain profile page.

FEDERATION_EXCEPTION_GET_PROVIDER_NAMES_UNDER_AUTH_DOMAIN

ID: CONSOLE-1163

Level: SEVERE

Description: Getting provider names under authentication domain failed.

Data: name of realm, name of authentication domain, error message

Triggers: Unable to get provider names under authentication domain due to federation SDK related errors.

Actions: Look under federation log for more information.

ATTEMPT_ADD_PROVIDERS_TO_AUTH_DOMAIN

ID: CONSOLE-1171

Level: INFO

Description: Attempt to add providers to an authentication domain

Data: name of realm, name of authentication domain, name of providers

Triggers: Click on Save button in provider assignment page.

SUCCEED_ADD_PROVIDERS_TO_AUTH_DOMAIN

ID: CONSOLE-1172

Level: INFO

Description: Addition of provider to an authentication domain succeeded.

Data: name of realm, name of authentication domain, name of providers

Triggers: Click on Save button in provider assignment page.

FEDERATION_EXCEPTION_ADD_PROVIDERS_TO_AUTH_DOMAIN

ID: CONSOLE-1173

Level: SEVERE

Description: Addition of provider to an authentication domain failed.

Data: name of realm, name of authentication domain, name of providers, error message

Triggers: Unable to add provider to authentication domain due to federation SDK related errors.

Actions: Look under federation log for more information.

ATTEMPT_REMOVE_PROVIDERS_FROM_AUTH_DOMAIN

ID: CONSOLE-1181

Level: INFO

Description: Attempt to remove providers from authentication domain

Data: name of realm, name of authentication domain, name of providers

Triggers: Click on Save button in provider assignment page.

SUCCEED_REMOVE_PROVIDERS_FROM_AUTH_DOMAIN

ID: CONSOLE-1182

Level: INFO

Description: Deletion of providers from authentication domain succeeded.

Data: name of realm, name of authentication domain, name of providers

Triggers: Click on Save button in provider assignment page.

FEDERATION_EXCEPTION_REMOVE_PROVIDERS_FROM_AUTH_DOMAIN

ID: CONSOLE-1183

Level: SEVERE

Description: Deletion of provider from authentication domain failed.

Data: name of realm, name of authentication domain, name of providers, error message

Triggers: Unable to remove provider from authentication domain due to federation SDK related errors.

Actions: Look under federation log for more information.

ATTEMPT_CREATE_PROVIDER

ID: CONSOLE-1301

Level: INFO

Description: Attempt to create provider

Data: name of provider, role of provider, type of provider

Triggers: Click on Save button in provider assignment page.

SUCCEED_CREATE_PROVIDER

ID: CONSOLE-1302

Level: INFO

Description: Creation of providers succeeded.

Data: name of provider, role of provider, type of provider

Triggers: Click on Save button in provider assignment page.

FEDERATION_EXCEPTION_CREATE_PROVIDER

ID: CONSOLE-1303

Level: SEVERE

Description: Creation of provider failed.

Data: name of provider, role of provider, type of provider, error message

Triggers: Unable to create provider due to federation SDK related errors.

Actions: Look under federation log for more information.

FEDERATION_EXCEPTION_CREATE_PROVIDER

ID: CONSOLE-1304

Level: SEVERE

Description: Creation of provider failed.

Data: name of provider, role of provider, type of provider, error message

Triggers: Unable to create provider due to federation SDK related errors.

Actions: Look under federation log for more information.

INVOCATION_TARGET_EXCEPTION_CREATE_PROVIDER

ID: CONSOLE-1305

Level: SEVERE

Description: Creation of provider failed.

Data: name of provider, role of provider, type of provider, error message

Triggers: Unable to create provider because Administration Console cannot find the appropriate methods to set values for this provider.

Actions: This is a web application error. Please contact Sun Support for assistant.

ATTEMPT_GET_PROVIDER_ATTRIBUTE_VALUES

ID: CONSOLE-1311

Level: INFO

Description: Attempt to get attribute values for provider

Data: name of provider, role of provider, type of provider

Triggers: View provider profile page.

SUCCEED_GET_PROVIDER_ATTRIBUTE_VALUES

ID: CONSOLE-1312

Level: INFO

Description: Getting attribute values of providers succeeded.

Data: name of provider, role of provider, type of provider

Triggers: View provider profile page.

ATTEMPT_GET_HANDLER_TO_PROVIDER

ID: CONSOLE-1321

Level: INFO

Description: Attempt to get handler to provider

Data: name of provider, role of provider

Triggers: View provider profile page.

SUCCEED_GET_HANDLER_TO_PROVIDER

ID: CONSOLE-1322

Level: INFO

Description: Getting handler to provider succeeded.

Data: name of provider, role of provider

Triggers: View provider profile page.

FEDERATION_EXCEPTION_GET_HANDLER_TO_PROVIDER

ID: CONSOLE-1323

Level: SEVERE

Description: Getting handler to provider failed.

Data: name of provider, role of provider, error message

Triggers: Unable to get handler to provider due to federation SDK related errors.

Actions: Look under federation log for more information.

ATTEMPT_MODIFY_PROVIDER

ID: CONSOLE-1331

Level: INFO

Description: Attempt to modify provider

Data: name of provider, role of provider

Triggers: Click on Save button in provider profile page.

SUCCEED_MODIFY_PROVIDER

ID: CONSOLE-1332

Level: INFO

Description: Modification of provider succeeded.

Data: name of provider, role of provider

Triggers: Click on Save button in provider profile page.

FEDERATION_EXCEPTION_MODIFY_PROVIDER

ID: CONSOLE-1333

Level: SEVERE

Description: Modification of provider failed.

Data: name of provider, role of provider, error message

Triggers: Unable to modify provider due to federation SDK related errors.

Actions: Look under federation log for more information.

INVOCATION_TARGET_EXCEPTION_MODIFY_PROVIDER

ID: CONSOLE-1334

Level: SEVERE

Description: Modification of provider failed.

Data: name of provider, role of provider, error message

Triggers: Unable to modify provider because Administration Console cannot find the appropriate methods to set values for this provider.

Actions: This is a web application error. Please contact Sun Support for assistant.

ATTEMPT_DELETE_PROVIDER

ID: CONSOLE-1341

Level: INFO

Description: Attempt to delete provider

Data: name of provider, role of provider

Triggers: Click on delete provider button in provider profile page.

SUCCEED_DELETE_PROVIDER

ID: CONSOLE-1342

Level: INFO

Description: Deletion of provider succeeded.

Data: name of provider, role of provider

Triggers: Click on delete provider button in provider profile page.

FEDERATION_EXCEPTION_DELETE_PROVIDER

ID: CONSOLE-1343

Level: SEVERE

Description: Deletion of provider failed.

Data: name of provider, role of provider, error message

Triggers: Unable to delete provider due to federation SDK related errors.

Actions: Look under federation log for more information.

ATTEMPT_GET_PROSPECTIVE_TRUSTED_PROVIDER

ID: CONSOLE-1351

Level: INFO

Description: Attempt to get prospective trusted provider

Data: name of provider, role of provider

Triggers: View add trusted provider page.

SUCCEED_GET_PROSPECTIVE_TRUSTED_PROVIDER

ID: CONSOLE-1352

Level: INFO

Description: Getting of prospective trusted provider succeeded.

Data: name of provider, role of provider

Triggers: View add trusted provider page.

FEDERATION_EXCEPTION_GET_PROSPECTIVE_TRUSTED_PROVIDER

ID: CONSOLE-1353

Level: SEVERE

Description: Getting of prospective trusted provider failed.

Data: name of provider, role of provider, error message

Triggers: Unable to get prospective trusted provider due to federation SDK related errors.

Actions: Look under federation log for more information.

ATTEMPT_GET_ATTR_VALUE_SCHEMA_TYPE

ID: CONSOLE-2001

Level: INFO

Description: Attempt to get attribute values of schema type of a service schema

Data: name of service, name of schema type, name of attribute schemas

Triggers: View service profile page.

SUCCEED_GET_ATTR_VALUE_SCHEMA_TYPE

ID: CONSOLE-2002

Level: INFO

Description: Getting attribute values of schema type of a service schema succeeded.

Data: name of service, name of schema type, name of attribute schemas

Triggers: View service profile page.

SSO_EXCEPTION_GET_ATTR_VALUE_SCHEMA_TYPE

ID: CONSOLE-2003

Level: SEVERE

Description: Getting attribute values of schema type of a service schema failed.

Data: name of service, name of schema type, name of attribute schemas, error message

Triggers: Unable to get attribute values of schema type of a service schema. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.

Actions: Look under service management log for more information.

SMS_EXCEPTION_GET_ATTR_VALUE_SCHEMA_TYPE

ID: CONSOLE-2004

Level: SEVERE

Description: Getting attribute values of schema type of a service schema failed.

Data: name of service, name of schema type, name of attribute schemas, error message

Triggers: Unable to get attribute values of schema type of a service schema due to service management SDK related errors.

Actions: Look under service management log for more information.

NO_SCHEMA_GET_ATTR_VALUE_SCHEMA_TYPE

ID: CONSOLE-2005

Level: INFO

Description: Getting attribute values of schema type of a service schema failed.

Data: name of service, name of schema type, name of attribute schemas

Triggers: View service profile page.

Actions: Need no action on this event. Console attempts to get a schema from a service but schema does not exist.

ATTEMPT_GET_ATTR_VALUE_ATR_SCHEMA_SCHEMA_TYPE

ID: CONSOLE-2011

Level: INFO

Description: Attempt to get attribute values of attribute schema of a schema type of a service schema

Data: name of service, name of schema type, name of attribute schemas

Triggers: View service profile page.

SUCCEED_GET_ATTR_VALUE_ATR_SCHEMA_SCHEMA_TYPE

ID: CONSOLE-2012

Level: INFO

Description: Getting attribute values of attribute schema of a schema type of a service schema succeeded.

Data: name of service, name of schema type, name of attribute schemas

Triggers: View service profile page.

SSO_EXCEPTION_GET_ATTR_VALUE_ATR_SCHEMA_SCHEMA_TYPE

ID: CONSOLE-2013

Level: SEVERE

Description: Getting attribute values of attribute schema of a schema type of a service schema failed.

Data: name of service, name of schema type, name of attribute schemas, error message

Triggers: Unable to get attribute values of schema type of a service schema. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.

Actions: Look under service management log for more information.

SMS_EXCEPTION_GET_ATTR_VALUE_ATR_SCHEMA_SCHEMA_TYPE

ID: CONSOLE-2014

Level: SEVERE

Description: Getting attribute values of attribute schema of a schema type of a service schema failed.

Data: name of service, name of schema type, name of attribute schemas, error message

Triggers: Unable to get attribute values of schema type of a service schema due to service management SDK related errors.

Actions: Look under service management log for more information.

ATTEMPT_SET_ATTR_VALUE_ATR_SCHEMA_SCHEMA_TYPE

ID: CONSOLE-2021

Level: INFO

Description: Attempt to modify attribute values of attribute schema of a schema type of a service schema

Data: name of service, name of schema type, name of attribute schemas

Triggers: Click on Save button in service profile page.

SUCCEED_SET_ATTR_VALUE_ATR_SCHEMA_SCHEMA_TYPE

ID: CONSOLE-2022

Level: INFO

Description: Modification attribute values of attribute schema of a schema type of a service schema succeeded.

Data: name of service, name of schema type, name of attribute schemas

Triggers: Click on Save button in service profile page.

SSO_EXCEPTION_SET_ATTR_VALUE_ATR_SCHEMA_SCHEMA_TYPE

ID: CONSOLE-2023

Level: SEVERE

Description: Modification attribute values of attribute schema of a schema type of a service schema failed.

Data: name of service, name of schema type, name of attribute schemas, error message

Triggers: Unable to modify attribute values of schema type of a service schema. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.

Actions: Look under service management log for more information.

SMS_EXCEPTION_SET_ATTR_VALUE_ATR_SCHEMA_SCHEMA_TYPE

ID: CONSOLE-2024

Level: SEVERE

Description: Modification attribute values of attribute schema of a schema type of a service schema failed.

Data: name of service, name of schema type, name of attribute schemas, error message

Triggers: Unable to modify attribute values of schema type of a service schema due to service management SDK related errors.

Actions: Look under service management log for more information.

ATTEMPT_GET_CURRENT_SESSIONS

ID: CONSOLE-3001

Level: INFO

Description: Attempt to get current sessions

Data: name of server, search pattern

Triggers: View session main page.

SUCCEED_GET_CURRENT_SESSIONS

ID: CONSOLE-3002

Level: INFO

Description: Getting of current sessions succeeded.

Data: name of server, search pattern

Triggers: View session main page.

SESSION_EXCEPTION_GET_CURRENT_SESSIONS

ID: CONSOLE-3003

Level: SEVERE

Description: Getting of current sessions failed.

Data: name of server, name of realm, error message

Triggers: Unable to get current sessions due to session SDK exception.

Actions: Look under session management log for more information.

ATTEMPT_INVALIDATE_SESSIONS

ID: CONSOLE-3011

Level: INFO

Description: Attempt to invalidate session

Data: name of server, ID of session

Triggers: Click on Invalidate button in session main page.

SUCCEED_INVALIDATE_SESSIONS

ID: CONSOLE-3012

Level: INFO

Description: Invalidation of session succeeded.

Data: name of server, ID of session

Triggers: Click on Invalidate button in session main page.

SESSION_EXCEPTION_INVALIDATE_SESSIONS

ID: CONSOLE-3013

Level: SEVERE

Description: Invalidation of session failed.

Data: name of server, ID of session, error message

Triggers: Unable to invalidate session due to session SDK exception.

Actions: Look under session management log for more information.

ATTEMPT_GET_SITE_NAMES

ID: CONSOLE-12001

Level: INFO

Description: Attempt to get site names

Data: server instance name

Triggers: View site and server management page.

SUCCEED_GET_SITE_NAMES

ID: CONSOLE-12002

Level: INFO

Description: Site names are returned.

Data: server instance name

Triggers: View site and server management page.

SSO_EXCEPTION_GET_SITE_NAMES

ID: CONSOLE-12003

Level: SEVERE

Description: Get site names.

Data: error message

Triggers: Unable to get site names. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.

Actions: Look under access management SDK log for more information.

SMS_EXCEPTION_GET_SITE_NAMES

ID: CONSOLE-12004

Level: SEVERE

Description: Get site names.

Data: error message

Triggers: Unable to get site names due the SMS API error.

Actions: Look under service management SDK log for more information.

ATTEMPT_GET_SITE_PRIMARY_URL

ID: CONSOLE-12011

Level: INFO

Description: Attempt to get primary URL of site.

Data: Site Name

Triggers: View site profile page.

SUCCEED_GET_SITE_PRIMARY_URL

ID: CONSOLE-12012

Level: INFO

Description: Primary URL of site is returned.

Data: Site Name

Triggers: View site profile page.

SSO_EXCEPTION_GET_SITE_PRIMARY_URL

ID: CONSOLE-12013

Level: SEVERE

Description: Get primary URL of site.

Data: Site Name, error message

Triggers: Unable to get primary URL of site. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.

Actions: Look under access management SDK log for more information.

SMS_EXCEPTION_GET_SITE_PRIMARY_URL

ID: CONSOLE-12014

Level: SEVERE

Description: Get primary URL of site.

Data: Site Name, error message

Triggers: Unable to get primary URL of site due the SMS API error.

Actions: Look under service management SDK log for more information.

ATTEMPT_GET_SITE_FAILOVER_URLS

ID: CONSOLE-12021

Level: INFO

Description: Attempt to get failover URLs of site.

Data: Site Name

Triggers: View site profile page.

SUCCEED_GET_SITE_FAILOVER_URLS

ID: CONSOLE-12022

Level: INFO

Description: Failover URLs of site is returned.

Data: Site Name

Triggers: View site profile page.

SSO_EXCEPTION_GET_SITE_FAILOVER_URLS

ID: CONSOLE-12023

Level: SEVERE

Description: Get failover URLs of site.

Data: Site Name, error message

Triggers: Unable to get failover URLs of site. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.

Actions: Look under access management SDK log for more information.

SMS_EXCEPTION_GET_SITE_FAILOVER_URLS

ID: CONSOLE-12024

Level: SEVERE

Description: Get failover URLs of site.

Data: Site Name, error message

Triggers: Unable to get failover URLs of site due the SMS API error.

Actions: Look under service management SDK log for more information.

ATTEMPT_GET_SITE_MEMBERS

ID: CONSOLE-12031

Level: INFO

Description: Attempt to get members of site.

Data: Site Name

Triggers: View site profile page.

SUCCEED_GET_SITE_MEMBERS

ID: CONSOLE-12032

Level: INFO

Description: Members of site is returned.

Data: Site Name

Triggers: View site profile page.

SSO_EXCEPTION_GET_SITE_MEMBERS

ID: CONSOLE-12033

Level: SEVERE

Description: Get members of site.

Data: Site Name, error message

Triggers: Unable to get members of site. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.

Actions: Look under access management SDK log for more information.

SMS_EXCEPTION_GET_SITE_MEMBERS

ID: CONSOLE-12034

Level: SEVERE

Description: Get members of site.

Data: Site Name, error message

Triggers: Unable to get members of site due the SMS API error.

Actions: Look under service management SDK log for more information.

ATTEMPT_CREATE_SITE

ID: CONSOLE-12041

Level: INFO

Description: Attempt to create site.

Data: Site Name

Triggers: View create site page.

SUCCEED_CREATE_SITE

ID: CONSOLE-12042

Level: INFO

Description: Site is created.

Data: Site Name

Triggers: Click on create button on creation page.

SSO_EXCEPTION_CREATE_SITE

ID: CONSOLE-12043

Level: SEVERE

Description: Create site.

Data: Site Name, error message

Triggers: Unable to create site. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.

Actions: Look under access management SDK log for more information.

SMS_EXCEPTION_CREATE_SITE

ID: CONSOLE-12044

Level: SEVERE

Description: Create site.

Data: Site Name, error message

Triggers: Unable to create site due the SMS API error.

Actions: Look under service management SDK log for more information.

ATTEMPT_CREATE_SERVER

ID: CONSOLE-12051

Level: INFO

Description: Attempt to create server.

Data: Server Name

Triggers: View create server page.

SUCCEED_CREATE_SERVER

ID: CONSOLE-12052

Level: INFO

Description: Server is created.

Data: Server Name

Triggers: Click on create button on creation page.

SSO_EXCEPTION_CREATE_SERVER

ID: CONSOLE-12053

Level: SEVERE

Description: Create server.

Data: Server Name, error message

Triggers: Unable to create server. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.

Actions: Look under access management SDK log for more information.

SMS_EXCEPTION_CREATE_SERVER

ID: CONSOLE-12054

Level: SEVERE

Description: Create server.

Data: Server Name, error message

Triggers: Unable to create server due the SMS API error.

Actions: Look under service management SDK log for more information.

CONFIGURATION_EXCEPTION_CREATE_SERVER

ID: CONSOLE-12055

Level: SEVERE

Description: Create server.

Data: Server Name, error message

Triggers: Unable to create server due the incorrect data format error.

Actions: Look under console log for more information.

IO_EXCEPTION_CREATE_SERVER

ID: CONSOLE-12056

Level: SEVERE

Description: Create server.

Data: Server Name, error message

Triggers: Unable to create server due the incorrect data format error.

Actions: Look under console log for more information.

ATTEMPT_DELETE_SITE

ID: CONSOLE-12061

Level: INFO

Description: Attempt to delete site.

Data: Site Name

Triggers: Click on delete site button.

SUCCEED_DELETE_SITE

ID: CONSOLE-12062

Level: INFO

Description: Site is deleted.

Data: Site Name

Triggers: Click on delete button.

SSO_EXCEPTION_DELETE_SITE

ID: CONSOLE-12063

Level: SEVERE

Description: Delete site.

Data: Site Name, error message

Triggers: Unable to delete site. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.

Actions: Look under access management SDK log for more information.

SMS_EXCEPTION_DELETE_SITE

ID: CONSOLE-12064

Level: SEVERE

Description: Delete site.

Data: Site Name, error message

Triggers: Unable to delete site due the SMS API error.

Actions: Look under service management SDK log for more information.

ATTEMPT_MODIFY_SITE

ID: CONSOLE-12071

Level: INFO

Description: Attempt to modify site.

Data: Site Name

Triggers: Click on OK button in site profile page.

SUCCEED_MODIFY_SITE

ID: CONSOLE-12072

Level: INFO

Description: Site is nodified.

Data: Site Name

Triggers: Click on OK button in site profile page.

SSO_EXCEPTION_MODIFY_SITE

ID: CONSOLE-12073

Level: SEVERE

Description: Modify site.

Data: Site Name, error message

Triggers: Unable to modify site. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.

Actions: Look under access management SDK log for more information.

SMS_EXCEPTION_MODIFY_SITE

ID: CONSOLE-12074

Level: SEVERE

Description: Modify site.

Data: Site Name, error message

Triggers: Unable to modify site due the SMS API error.

Actions: Look under service management SDK log for more information.

CONFIGURATION_EXCEPTION_MODIFY_SITE

ID: CONSOLE-12075

Level: SEVERE

Description: Modify site.

Data: Site Name, error message

Triggers: Unable to modify site due the incorrect data format.

Actions: Look under console log for more information.

ATTEMPT_GET_SERVER_NAMES

ID: CONSOLE-12081

Level: INFO

Description: Attempt to get server names.

Data: server instance name

Triggers: View site and server management page.

SUCCEED_GET_SERVER_NAMES

ID: CONSOLE-12082

Level: INFO

Description: Server names are returned.

Data: server instance name

Triggers: View site and server management page.

SSO_EXCEPTION_GET_SERVER_NAMES

ID: CONSOLE-12083

Level: SEVERE

Description: Get server name.

Data: error message

Triggers: Unable to get server names. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.

Actions: Look under access management SDK log for more information.

SMS_EXCEPTION_GET_SERVER_NAMES

ID: CONSOLE-12084

Level: SEVERE

Description: Get server name.

Data: error message

Triggers: Unable to get server names due the SMS API error.

Actions: Look under service management SDK log for more information.

ATTEMPT_GET_SERVER_SITE

ID: CONSOLE-12091

Level: INFO

Description: Attempt to get server's site.

Data: Server Name

Triggers: View server profile page.

SUCCEED_GET_SERVER_SITE

ID: CONSOLE-12092

Level: INFO

Description: Server's site name is returned.

Data: Server Name

Triggers: View server profile page.

SSO_EXCEPTION_GET_SERVER_SITE

ID: CONSOLE-12093

Level: SEVERE

Description: Get server's site name.

Data: Server Name, error message

Triggers: Unable to get server's site. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.

Actions: Look under access management SDK log for more information.

SMS_EXCEPTION_GET_SERVER_SITE

ID: CONSOLE-12094

Level: SEVERE

Description: Get server's site name.

Data: Server Name, error message

Triggers: Unable to get server's site due the SMS API error.

Actions: Look under service management SDK log for more information.

ATTEMPT_DELETE_SERVER

ID: CONSOLE-12101

Level: INFO

Description: Attempt to delete server.

Data: Server Name

Triggers: Click on delete button in server management page.

SUCCEED_DELETE_SERVER

ID: CONSOLE-12102

Level: INFO

Description: Server is delete.

Data: Server Name

Triggers: Click on delete button in server management page.

SSO_EXCEPTION_DELETE_SERVER

ID: CONSOLE-12103

Level: SEVERE

Description: Delete server.

Data: Server Name, error message

Triggers: Unable to delete server. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.

Actions: Look under access management SDK log for more information.

SMS_EXCEPTION_DELETE_SERVER

ID: CONSOLE-12104

Level: SEVERE

Description: Delete server.

Data: Server Name, error message

Triggers: Unable to delete server due the SMS API error.

Actions: Look under service management SDK log for more information.

ATTEMPT_CLONE_SERVER

ID: CONSOLE-12201

Level: INFO

Description: Attempt to clone server.

Data: Server Name, Cloned Server Name

Triggers: Click on clone button in server management page.

SUCCEED_CLONE_SERVER

ID: CONSOLE-12202

Level: INFO

Description: Server is cloned.

Data: Server Name, Cloned Server Name

Triggers: Click on clone button in server management page.

SSO_EXCEPTION_CLONE_SERVER

ID: CONSOLE-12203

Level: SEVERE

Description: clone server.

Data: Server Name, Cloned Server Name, error message

Triggers: Unable to clone server. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.

Actions: Look under access management SDK log for more information.

SMS_EXCEPTION_CLONE_SERVER

ID: CONSOLE-12204

Level: SEVERE

Description: clone server.

Data: Server Name, Cloned Server Name, error message

Triggers: Unable to clone server due the SMS API error.

Actions: Look under service management SDK log for more information.

CONFIGURATION_EXCEPTION_CLONE_SERVER

ID: CONSOLE-12205

Level: SEVERE

Description: clone server.

Data: Server Name, Cloned Server Name, error message

Triggers: Unable to clone server due the data format error.

Actions: Look under console log for more information.

ATTEMPT_GET_SERVER_CONFIG

ID: CONSOLE-12211

Level: INFO

Description: Attempt to get server's configuration.

Data: Server Name

Triggers: View server profile page.

SUCCEED_GET_SERVER_CONFIG

ID: CONSOLE-12212

Level: INFO

Description: Server's configuration is returned.

Data: Server Name

Triggers: View server profile page.

SSO_EXCEPTION_GET_SERVER_CONFIG

ID: CONSOLE-12213

Level: SEVERE

Description: Get server's configuration.

Data: Server Name, error message

Triggers: Unable to get server's configuration. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.

Actions: Look under access management SDK log for more information.

SMS_EXCEPTION_GET_SERVER_CONFIG

ID: CONSOLE-12214

Level: SEVERE

Description: Get server's configuration.

Data: Server Name, error message

Triggers: Unable to get server's configuration due the SMS API error.

Actions: Look under service management SDK log for more information.

IO_EXCEPTION_GET_SERVER_CONFIG

ID: CONSOLE-12215

Level: SEVERE

Description: get server's configuration.

Data: Server Name, error message

Triggers: Unable to get server's configuration due the data parsing error.

Actions: Look under console log for more information.

ATTEMPT_GET_SERVER_DEFAULT_CONFIG

ID: CONSOLE-12221

Level: INFO

Description: Attempt to get server default configuration.

Data: server instance name

Triggers: View server profile page.

SUCCEED_GET_SERVER_DEFAULT_CONFIG

ID: CONSOLE-12222

Level: INFO

Description: Server default configuration is returned.

Data: server instance name

Triggers: View server profile page.

ATTEMPT_MODIFY_SERVER

ID: CONSOLE-12231

Level: INFO

Description: Attempt to modify server.

Data: Server Name

Triggers: Click on OK button in server profile page.

SUCCEED_MODIFY_SERVER

ID: CONSOLE-12232

Level: INFO

Description: Server is modified.

Data: Server Name

Triggers: Click on OK button in server profile page.

SSO_EXCEPTION_MODIFY_SERVER

ID: CONSOLE-12233

Level: SEVERE

Description: modify server.

Data: Server Name, error message

Triggers: Unable to modify server. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.

Actions: Look under access management SDK log for more information.

SMS_EXCEPTION_MODIFY_SERVER

ID: CONSOLE-12234

Level: SEVERE

Description: modify server.

Data: Server Name, error message

Triggers: Unable to modify server due the SMS API error.

Actions: Look under service management SDK log for more information.

IO_EXCEPTION_MODIFY_SERVER

ID: CONSOLE-12235

Level: SEVERE

Description: modify server.

Data: Server Name, error message

Triggers: Unable to modify server due the data parsing error.

Actions: Look under console log for more information.

CONFIGURATION_EXCEPTION_MODIFY_SERVER

ID: CONSOLE-12236

Level: SEVERE

Description: modify server.

Data: Server Name, error message

Triggers: Unable to modify server due the incorrect data format error.

Actions: Look under console log for more information.

ATTEMPT_MODIFY_SERVER_INHERITANCE

ID: CONSOLE-12241

Level: INFO

Description: Attempt to modify server's inheritance.

Data: Server Name

Triggers: Click on OK button in server inheritance setting page.

SUCCEED_MODIFY_SERVER_INHERITANCE

ID: CONSOLE-12242

Level: INFO

Description: Server's inheritance setting is modified.

Data: Server Name

Triggers: Click on OK button in server inheritance setting page.

SSO_EXCEPTION_MODIFY_SERVER_INHERITANCE

ID: CONSOLE-12243

Level: SEVERE

Description: Modify server's inheritance.

Data: Server Name, error message

Triggers: Unable to modify server's inheritance. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.

Actions: Look under access management SDK log for more information.

SMS_EXCEPTION_MODIFY_SERVER_INHERITANCE

ID: CONSOLE-12244

Level: SEVERE

Description: Modify server's inheritance.

Data: Server Name, error message

Triggers: Unable to modify server's inheritance due the SMS API error.

Actions: Look under service management SDK log for more information.

IO_EXCEPTION_MODIFY_SERVER_INHERITANCE

ID: CONSOLE-12245

Level: SEVERE

Description: modify server's inheritance.

Data: Server Name, error message

Triggers: Unable to modify server's inheritance due the data parsing error.

Actions: Look under console log for more information.

CONFIGURATION_EXCEPTION_MODIFY_SERVER_INHERITANCE

ID: CONSOLE-12246

Level: SEVERE

Description: modify server's inheritance.

Data: Server Name, error message

Triggers: Unable to modify server's inheritance due the incorrect data format error.

Actions: Look under console log for more information.

ATTEMPT_GET_SERVER_CONFIG_XML

ID: CONSOLE-12251

Level: INFO

Description: Attempt to get server's configuration XML.

Data: Server Name

Triggers: View server's server configuration XML profile page.

SUCCEED_GET_SERVER_CONFIG_XML

ID: CONSOLE-12252

Level: INFO

Description: Server's configuration XML is returned.

Data: Server Name

Triggers: View server's server configuration XML profile page.

SSO_EXCEPTION_GET_SERVER_CONFIG_XML

ID: CONSOLE-12253

Level: SEVERE

Description: Get server's configuration XML.

Data: Server Name, error message

Triggers: Unable to get server's configuration XML. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.

Actions: Look under access management SDK log for more information.

SMS_EXCEPTION_GET_SERVER_CONFIG_XML

ID: CONSOLE-12254

Level: SEVERE

Description: sGget server's configuration XML.

Data: Server Name, error message

Triggers: Unable to get server's configuration XML due the SMS API error.

Actions: Look under service management SDK log for more information.

GENERIC_EXCEPTION_GET_SERVER_CONFIG_XML

ID: CONSOLE-12255

Level: SEVERE

Description: sGget server's configuration XML.

Data: Server Name, error message

Triggers: Unable to get server's configuration XML due the data parsing error.

Actions: Look under console log for more information.

ATTEMPT_SET_SERVER_CONFIG_XML

ID: CONSOLE-12261

Level: INFO

Description: Attempt to set server's configuration XML.

Data: Server Name

Triggers: Click on OK button in server's server configuration XML profile page.

SUCCEED_SET_SERVER_CONFIG_XML

ID: CONSOLE-12262

Level: INFO

Description: Server's configuration XML is modified.

Data: Server Name

Triggers: Click on OK button in server's server configuration XML profile page.

SSO_EXCEPTION_SET_SERVER_CONFIG_XML

ID: CONSOLE-12263

Level: SEVERE

Description: set server's configuration XML.

Data: Server Name, error message

Triggers: Unable to set server's configuration XML. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.

Actions: Look under access management SDK log for more information.

SMS_EXCEPTION_SET_SERVER_CONFIG_XML

ID: CONSOLE-12264

Level: SEVERE

Description: sGset server's configuration XML.

Data: Server Name, error message

Triggers: Unable to set server's configuration XML due the SMS API error.

Actions: Look under service management SDK log for more information.

ATTEMPT_SEARCH_AGENT

ID: CONSOLE-13001

Level: INFO

Description: Attempt to search for agents

Data: base realm, agent type, search pattern, search size limit, search time limit

Triggers: Click on Search button in agent search view.

SUCCEED_SEARCH_AGENT

ID: CONSOLE-13002

Level: INFO

Description: Searching for agents succeeded

Data: base realm, agent type, search pattern, search size limit, search time limit

Triggers: Click on Search button in agent search view.

EXCEPTION_SEARCH_AGENT

ID: CONSOLE-13003

Level: SEVERE

Description: Searching for agents failed

Data: base realm, agent type, search pattern, search size limit, search time limit, error message

Triggers: Unable to perform search operation on agents under a realm. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.

Actions: Look under data store log for more information.

ATTEMPT_DELETE_AGENT

ID: CONSOLE-13011

Level: INFO

Description: Attempt to delete agents

Data: base realm, agent names

Triggers: Click on Delete button in agent home page.

SUCCEED_DELETE_AGENT

ID: CONSOLE-13012

Level: INFO

Description: Agents are deleted

Data: base realm, agent names

Triggers: Click on Delete button in agent home page.

EXCEPTION_DELETE_AGENT

ID: CONSOLE-13013

Level: SEVERE

Description: Deletion of agents failed

Data: base realm, agent names, error message

Triggers: Unable to perform delete operation on agents under a realm. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.

Actions: Look under data store log for more information.

ATTEMPT_SEARCH_AGENT_GROUP

ID: CONSOLE-13021

Level: INFO

Description: Attempt to search for agent groups

Data: base realm, agent type, search pattern, search size limit, search time limit

Triggers: Click on Search button in agent search view.

SUCCEED_SEARCH_AGENT_GROUP

ID: CONSOLE-13022

Level: INFO

Description: Searching for agent groups succeeded

Data: base realm, agent type, search pattern, search size limit, search time limit

Triggers: Click on Search button in agent search view.

EXCEPTION_SEARCH_AGENT_GROUP

ID: CONSOLE-13023

Level: SEVERE

Description: Searching for agent groups failed

Data: base realm, agent type, search pattern, search size limit, search time limit, error message

Triggers: Unable to perform search operation on agent groups under a realm. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.

Actions: Look under data store log for more information.

ATTEMPT_DELETE_AGENT_GROUP

ID: CONSOLE-13031

Level: INFO

Description: Attempt to delete agent groups

Data: base realm, agent group names

Triggers: Click on Delete button in agent home page.

SUCCEED_DELETE_AGENT_GROUP

ID: CONSOLE-13032

Level: INFO

Description: Agent groups are deleted

Data: base realm, agent group names

Triggers: Click on Delete button in agent home page.

EXCEPTION_DELETE_AGENT_GROUP

ID: CONSOLE-13033

Level: SEVERE

Description: Deletion of agent groups failed

Data: base realm, agent group names, error message

Triggers: Unable to perform delete operation on agents under a realm. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.

Actions: Look under data store log for more information.

ATTEMPT_CREATE_AGENT

ID: CONSOLE-13041

Level: INFO

Description: Attempt to create agent

Data: base realm, agent name, agent type

Triggers: Click on New button in agent home page.

SUCCEED_CREATE_AGENT

ID: CONSOLE-13042

Level: INFO

Description: Agent is created

Data: base realm, agent name, agent type

Triggers: Click on New button in agent home page.

EXCEPTION_CREATE_AGENT

ID: CONSOLE-13043

Level: SEVERE

Description: Creation of agent failed

Data: base realm, agent name, agent type, error message

Triggers: Unable to perform create agent. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.

Actions: Look under data store log for more information.

ATTEMPT_CREATE_AGENT_GROUP

ID: CONSOLE-13051

Level: INFO

Description: Attempt to create agent group

Data: base realm, agent group name, agent type

Triggers: Click on New button in agent home page.

SUCCEED_CREATE_AGENT_GROUP

ID: CONSOLE-13052

Level: INFO

Description: Agent group is created

Data: base realm, agent group name, agent type

Triggers: Click on New button in agent home page.

EXCEPTION_CREATE_AGENT_GROUP

ID: CONSOLE-13053

Level: SEVERE

Description: Creation of agent group failed

Data: base realm, agent group name, agent type, error message

Triggers: Unable to perform create agent group. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.

Actions: Look under data store log for more information.

ATTEMPT_GET_AGENT_ATTRIBUTE_VALUES

ID: CONSOLE-13061

Level: INFO

Description: Attempt to get agent attribute values

Data: agent universal Id

Triggers: Visit agent profile page.

SUCCEED_GET_AGENT_ATTRIBUTE_VALUES

ID: CONSOLE-13062

Level: INFO

Description: Agent attribute values is retrieved.

Data: agent universal Id

Triggers: Visit agent profile page.

EXCEPTION_GET_AGENT_ATTRIBUTE_VALUES

ID: CONSOLE-13063

Level: SEVERE

Description: Unable to get agent attribute values

Data: agent universal Id, error message

Triggers: Unable to perform get agent attribute values. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.

Actions: Look under data store log for more information.

ATTEMPT_SET_AGENT_ATTRIBUTE_VALUE

ID: CONSOLE-13071

Level: INFO

Description: Attempt to set agent attribute values

Data: agent universal Id

Triggers: Click on save button in agent profile page.

SUCCEED_SET_AGENT_ATTRIBUTE_VALUE

ID: CONSOLE-13072

Level: INFO

Description: Agent attribute values set successfully

Data: agent universal Id

Triggers: Click on save button in agent profile page.

EXCEPTION_SET_AGENT_ATTRIBUTE_VALUE

ID: CONSOLE-13073

Level: SEVERE

Description: Unable to set agent attribute values

Data: agent universal Id, error message

Triggers: Unable to perform set agent attribute values. It may be the single sign on token of the user has expired; or the user does not have permission to perform this operation.

Actions: Look under data store log for more information.

ATTEMPT_GET_ATTR_VALUES_OF_SESSION_HA_PROPERTIES

ID: CONSOLE-13074

Level: INFO

Description: Attempt to read session HA properties

Data: name of attribute

Triggers: Click on Save button in session profile page.

SUCCEED_GET_ATTR_VALUES_OF_SESSION_HA_PROPERTIES

ID: CONSOLE-13075

Level: INFO

Description: Read Access of session HA properties succeeded.

Data: name of attribute

Triggers: Click on Save button in session profile page.

SMS_EXCEPTION_GET_ATTR_VALUES_OF_SESSION_HA_PROPERTIES

ID: CONSOLE-13076

Level: SEVERE

Description: Read Access of session HA properties failed.

Data: name of attribute, error message

Triggers: Unable to modify session HA properties due to service management SDK exception.

Actions: Look under service management log for more information.

ATTEMPT_SET_ATTR_VALUES_OF_SESSION_HA_PROPERTIES

ID: CONSOLE-13077

Level: INFO

Description: Attempt to modify session HA properties

Data: name of attribute

Triggers: Click on Save button in session profile page.

SUCCEED_SET_ATTR_VALUES_OF_SESSION_HA_PROPERTIES

ID: CONSOLE-13078

Level: INFO

Description: Modification of session HA properties succeeded.

Data: name of attribute

Triggers: Click on Save button in session profile page.

SMS_EXCEPTION_SET_ATTR_VALUES_OF_SESSION_HA_PROPERTIES

ID: CONSOLE-13079

Level: SEVERE

Description: Modification of session HA properties failed.

Data: name of attribute, error message

Triggers: Unable to modify session HA properties due to service management SDK exception.

Actions: Look under service management log for more information.

ATTEMPT_GET_AFFILIATION_ATTR_VALUES

ID: CONSOLE-13101

Level: INFO

Description: Attempt to get attribute values of an affiliation.

Data: descriptor realm, descriptor name, descriptor protocol, descriptor type

Triggers: View SAMLv2 Affiliate page.

SUCCEED_GET_AFFILIATION_ATTR_VALUES

ID: CONSOLE-13102

Level: INFO

Description: Getting attribute values of affiliation succeeded.

Data: descriptor realm, descriptor name, descriptor protocol, descriptor type

Triggers: View SAMLv2 Affiliate page.

FEDERATION_EXCEPTION_GET_AFFILIATION_ATTR_VALUES

ID: CONSOLE-13103

Level: SEVERE

Description: Getting attribute values of affiliation failed.

Data: descriptor realm, descriptor name, descriptor protocol, descriptor type, error message

Triggers: Unable to get attribute values of affiliation due to federation SDK related errors.

Actions: Look under federation log for more information.

ATTEMPT_MODIFY_AFFILIATION_ATTR_VALUES

ID: CONSOLE-13111

Level: INFO

Description: Attempt to modify affiliation.

Data: descriptor realm, descriptor name, descriptor protocol, descriptor type

Triggers: Click on Save button in SAMLv2 Affiliate page.

SUCCEED_MODIFY_AFFILIATION_ATTR_VALUES

ID: CONSOLE-13112

Level: INFO

Description: Modification of affiliation succeeded.

Data: descriptor realm, descriptor name, descriptor protocol, descriptor type

Triggers: Click on Save button in SAMLv2 Affiliate page.

FEDERATION_EXCEPTION_MODIFY_AFFILIATION_ATTR_VALUES

ID: CONSOLE-13113

Level: SEVERE

Description: Modification of affiliation failed.

Data: descriptor realm, descriptor name, descriptor protocol, descriptor type, error message

Triggers: Unable to modify affiliation due to federation SDK related errors.

Actions: Look under federation log for more information.

ATTEMPT_GET_ATTR_AUTH_ATTR_VALUES

ID: CONSOLE-13121

Level: INFO

Description: Attempt to get attribute values of an attribute authority.

Data: descriptor realm, descriptor name, descriptor protocol, descriptor type

Triggers: View SAMLv2 AttrAuthority page.

SUCCEED_GET_ATTR_AUTH_ATTR_VALUES

ID: CONSOLE-13122

Level: INFO

Description: Getting attribute values of attribute authority succeeded.

Data: descriptor realm, descriptor name, descriptor protocol, descriptor type

Triggers: View SAMLv2 AttrAuthority page.

FEDERATION_EXCEPTION_GET_ATTR_AUTH_ATTR_VALUES

ID: CONSOLE-13123

Level: SEVERE

Description: Getting attribute values of attribute authority failed.

Data: descriptor realm, descriptor name, descriptor protocol, descriptor type, error message

Triggers: Unable to get attribute values of attribute authority due to federation SDK related errors.

Actions: Look under federation log for more information.

ATTEMPT_MODIFY_ATTR_AUTH_ATTR_VALUES

ID: CONSOLE-13131

Level: INFO

Description: Attempt to modify attribute authority.

Data: descriptor realm, descriptor name, descriptor protocol, descriptor type

Triggers: Click on Save button in SAMLv2 AttrAuthority page.

SUCCEED_MODIFY_ATTR_AUTH_ATTR_VALUES

ID: CONSOLE-13132

Level: INFO

Description: Modification of attribute authority succeeded.

Data: descriptor realm, descriptor name, descriptor protocol, descriptor type

Triggers: Click on Save button in SAMLv2 AttrAuthority page.

FEDERATION_EXCEPTION_MODIFY_ATTR_AUTH_ATTR_VALUES

ID: CONSOLE-13133

Level: SEVERE

Description: Modification of attribute authority failed.

Data: descriptor realm, descriptor name, descriptor protocol, descriptor type, error message

Triggers: Unable to modify attribute authority due to federation SDK related errors.

Actions: Look under federation log for more information.

ATTEMPT_GET_ATTR_QUERY_ATTR_VALUES

ID: CONSOLE-13141

Level: INFO

Description: Attempt to get attribute values of an attribute query.

Data: descriptor realm, descriptor name, descriptor protocol, descriptor type

Triggers: View SAMLv2 AttrQuery page.

SUCCEED_GET_ATTR_QUERY_ATTR_VALUES

ID: CONSOLE-13142

Level: INFO

Description: Getting attribute values of attribute query succeeded.

Data: descriptor realm, descriptor name, descriptor protocol, descriptor type

Triggers: View SAMLv2 AttrQuery page.

FEDERATION_EXCEPTION_GET_ATTR_QUERY_ATTR_VALUES

ID: CONSOLE-13143

Level: SEVERE

Description: Getting attribute values of attribute query failed.

Data: descriptor realm, descriptor name, descriptor protocol, descriptor type, error message

Triggers: Unable to get attribute values of attribute query due to federation SDK related errors.

Actions: Look under federation log for more information.

ATTEMPT_MODIFY_ATTR_QUERY_ATTR_VALUES

ID: CONSOLE-13151

Level: INFO

Description: Attempt to modify attribute query.

Data: descriptor realm, descriptor name, descriptor protocol, descriptor type

Triggers: Click on Save button in SAMLv2 AttrQuery page.

SUCCEED_MODIFY_ATTR_QUERY_ATTR_VALUES

ID: CONSOLE-13152

Level: INFO

Description: Modification of attribute query succeeded.

Data: descriptor realm, descriptor name, descriptor protocol, descriptor type

Triggers: Click on Save button in SAMLv2 AttrQuery page.

FEDERATION_EXCEPTION_MODIFY_ATTR_QUERY_ATTR_VALUES

ID: CONSOLE-13153

Level: SEVERE

Description: Modification of attribute query failed.

Data: descriptor realm, descriptor name, descriptor protocol, descriptor type, error message

Triggers: Unable to modify attribute query due to federation SDK related errors.

Actions: Look under federation log for more information.

ATTEMPT_GET_AUTHN_AUTH_ATTR_VALUES

ID: CONSOLE-13161

Level: INFO

Description: Attempt to get attribute values of an authn authority.

Data: descriptor realm, descriptor name, descriptor protocol, descriptor type

Triggers: View SAMLv2 AuthnAuthority page.

SUCCEED_GET_AUTHN_AUTH_ATTR_VALUES

ID: CONSOLE-13162

Level: INFO

Description: Getting attribute values of authn authority succeeded.

Data: descriptor realm, descriptor name, descriptor protocol, descriptor type

Triggers: View SAMLv2 AuthnAuthority page.

FEDERATION_EXCEPTION_GET_AUTHN_AUTH_ATTR_VALUES

ID: CONSOLE-13163

Level: SEVERE

Description: Getting attribute values of authn authority failed.

Data: descriptor realm, descriptor name, descriptor protocol, descriptor type, error message

Triggers: Unable to get attribute values of authn authority due to federation SDK related errors.

Actions: Look under federation log for more information.

ATTEMPT_MODIFY_AUTHN_AUTH_ATTR_VALUES

ID: CONSOLE-13171

Level: INFO

Description: Attempt to modify authn authority.

Data: descriptor realm, descriptor name, descriptor protocol, descriptor type

Triggers: Click on Save button in SAMLv2 AuthnAuthority page.

SUCCEED_MODIFY_AUTHN_AUTH_ATTR_VALUES

ID: CONSOLE-13172

Level: INFO

Description: Modification of authn authority succeeded.

Data: descriptor realm, descriptor name, descriptor protocol, descriptor type

Triggers: Click on Save button in SAMLv2 AuthnAuthority page.

FEDERATION_EXCEPTION_MODIFY_AUTHN_AUTH_ATTR_VALUES

ID: CONSOLE-13173

Level: SEVERE

Description: Modification of authn authority failed.

Data: descriptor realm, descriptor name, descriptor protocol, descriptor type, error message

Triggers: Unable to modify authn authority due to federation SDK related errors.

Actions: Look under federation log for more information.

ATTEMPT_GET_METAALIAS

ID: CONSOLE-13181

Level: INFO

Description: Attempt to get a meta alias.

Data: descriptor realm, descriptor name, descriptor protocol, descriptor type

Triggers: View SAMLv2 IDP Services page.

SUCCEED_GET_METAALIAS

ID: CONSOLE-13182

Level: INFO

Description: Getting meta alias succeeded.

Data: descriptor realm, descriptor name, descriptor protocol, descriptor type

Triggers: View SAMLv2 IDP Services page.

FEDERATION_EXCEPTION_GET_METAALIAS

ID: CONSOLE-13183

Level: SEVERE

Description: Getting meta alias failed.

Data: descriptor realm, descriptor name, descriptor protocol, descriptor type, error message

Triggers: Unable to get meta alias due to federation SDK related errors.

Actions: Look under federation log for more information.

OpenAM logs the following ENTITLEMENT messages.

ATTEMPT_ADD_PRIVILEGE

ID: ENTITLEMENT-1

Level: INFO

Description: Attempt to add privilege.

Data: realm, privilege name

Triggers: Add privilege API is called.

SUCCEEDED_ADD_PRIVILEGE

ID: ENTITLEMENT-2

Level: INFO

Description: Privilege is added.

Data: realm, privilege name

Triggers: Add privilege API is called.

FAILED_ADD_PRIVILEGE

ID: ENTITLEMENT-3

Level: INFO

Description: Failed to add privilege.

Data: realm, privilege name, error message

Triggers: Add privilege API is called.

Actions: Privilege might already exists.; Administrator might not have the permission to add privilege.

ATTEMPT_ADD_REFERRAL

ID: ENTITLEMENT-11

Level: INFO

Description: Attempt to add referral privilege.

Data: realm, privilege name

Triggers: Add referral privilege API is called.

SUCCEEDED_ADD_REFERRAL

ID: ENTITLEMENT-12

Level: INFO

Description: Referral Privilege is added.

Data: realm, privilege name

Triggers: Add referral privilege API is called.

FAILED_ADD_REFERRAL

ID: ENTITLEMENT-13

Level: INFO

Description: Failed to add referral privilege.

Data: realm, privilege name, error message

Triggers: Add referral privilege API is called.

Actions: Privilege might already exists.; Administrator might not have the permission to add referral privilege.

ATTEMPT_REMOVE_PRIVILEGE

ID: ENTITLEMENT-21

Level: INFO

Description: Attempt to remove privilege.

Data: realm, privilege name

Triggers: Remove privilege API is called.

SUCCEEDED_REMOVE_PRIVILEGE

ID: ENTITLEMENT-22

Level: INFO

Description: Privilege is removed.

Data: realm, privilege name

Triggers: Removed privilege API is called.

FAILED_REMOVE_PRIVILEGE

ID: ENTITLEMENT-23

Level: INFO

Description: Failed to removed privilege.

Data: realm, privilege name, error message

Triggers: Removed privilege API is called.

Actions: Administrator might not have the permission to remove privilege.

ATTEMPT_REMOVE_REFERRAL

ID: ENTITLEMENT-31

Level: INFO

Description: Attempt to remove referral privilege.

Data: realm, privilege name

Triggers: Remove referral privilege API is called.

SUCCEEDED_REMOVE_REFERRAL

ID: ENTITLEMENT-32

Level: INFO

Description: Referral privilege is removed.

Data: realm, privilege name

Triggers: Removed referral privilege API is called.

FAILED_REMOVE_REFERRAL

ID: ENTITLEMENT-33

Level: INFO

Description: Failed to removed referral privilege.

Data: realm, privilege name, error message

Triggers: Removed referral privilege API is called.

Actions: Administrator might not have the permission to remove privilege.

ATTEMPT_SAVE_APPLICATION

ID: ENTITLEMENT-101

Level: INFO

Description: Attempt to save application.

Data: realm, application name

Triggers: Save application API is called.

SUCCEEDED_SAVE_APPLICATION

ID: ENTITLEMENT-102

Level: INFO

Description: Application is saved.

Data: realm, application name

Triggers: Save application API is called.

FAILED_SAVE_APPLICATION

ID: ENTITLEMENT-103

Level: INFO

Description: Failed to save application.

Data: realm, application name, error message

Triggers: Save application API is called.

Actions: Administrator might not have the permission to save application.

ATTEMPT_REMOVE_APPLICATION

ID: ENTITLEMENT-111

Level: INFO

Description: Attempt to remove application.

Data: realm, application name

Triggers: Remove application API is called.

SUCCEEDED_REMOVE_APPLICATION

ID: ENTITLEMENT-112

Level: INFO

Description: Application is removed.

Data: realm, application name

Triggers: Remove application API is called.

FAILED_REMOVE_APPLICATION

ID: ENTITLEMENT-113

Level: INFO

Description: Failed to remove application.

Data: realm, application name, error message

Triggers: Remove application API is called.

Actions: Administrator might not have the permission to remove application.

ATTEMPT_SAVE_RESOURCE_TYPE

ID: ENTITLEMENT-40

Level: INFO

Description: Attempt to save resource type.

Data: realm, resource type name

Triggers: Save resource type API is called.

SUCCEEDED_SAVE_RESOURCE_TYPE

ID: ENTITLEMENT-41

Level: INFO

Description: Resource type is saved.

Data: realm, resource type name

Triggers: Save resource type API is called.

FAILED_SAVE_RESOURCE_TYPE

ID: ENTITLEMENT-42

Level: INFO

Description: Failed to save resource type.

Data: realm, resource type name, error message

Triggers: Save resource type API is called.

Actions: Administrator might not have the permission to save resource type.

ATTEMPT_REMOVE_RESOURCE_TYPE

ID: ENTITLEMENT-43

Level: INFO

Description: Attempt to remove resource type.

Data: realm, resource type name

Triggers: Remove resource type API is called.

SUCCEEDED_REMOVE_RESOURCE_TYPE

ID: ENTITLEMENT-44

Level: INFO

Description: Resource type is removed.

Data: realm, resource type name

Triggers: Remove resource type API is called.

FAILED_REMOVE_RESOURCE_TYPE

ID: ENTITLEMENT-45

Level: INFO

Description: Failed to remove resource type.

Data: realm, resource type name, error message

Triggers: Remove resource type API is called.

Actions: Administrator might not have the permission to remove resource type.

OpenAM logs the following LOG messages.

LOG_START_NEW_LOGGER

ID: LOG-1

Level: INFO

Description: Logging Started - New Logger

Data: current location

Triggers: Logging started by getting a new Logger.

LOG_END

ID: LOG-2

Level: INFO

Description: Logging Terminated - Server Stopped

Data: current location

Triggers: Logging terminated by server shutdown.

LOG_START_CONFIG

ID: LOG-3

Level: INFO

Description: Logging Started - Configuration Change

Data: old location, new location, old backend, new backend, old security status, new security status, old status, new status, old level, new level

Triggers: Logging started after logging configuration change.

LOG_END_CONFIG

ID: LOG-4

Level: INFO

Description: Logging Terminated - Configuration Change

Data: old location, new location, old backend, new backend, old security status, new security status, old status, new status, old level, new level

Triggers: Logging terminated by logging configuration change.

OpenAM logs the following OAuth2Provider messages.

CREATED_TOKEN

ID: OAuth2Provider-1

Level: INFO

Description: Created an oauth 2.0 token

Data: message, token info

Triggers: Created a new oauth 2.0 token

DELETED_TOKEN

ID: OAuth2Provider-2

Level: INFO

Description: Deleted an oauth 2.0 token

Data: message, token info

Triggers: Deleted an oauth 2.0 token

FAILED_CREATE_TOKEN

ID: OAuth2Provider-3

Level: INFO

Description: Failed to creating an oauth 2.0 token

Data: message, token info

Triggers: Failed creating an oauth 2.0 token

FAILED_DELETE_TOKEN

ID: OAuth2Provider-4

Level: INFO

Description: Failed deleting an oauth 2.0 token

Data: message, token info

Triggers: Failed deleting an oauth 2.0 token

CREATED_REFRESH_TOKEN

ID: OAuth2Provider-5

Level: INFO

Description: Created an oauth 2.0 refresh token

Data: message, token info

Triggers: Created an oauth 2.0 refresh token

FAILED_CREATE_REFRESH_TOKEN

ID: OAuth2Provider-6

Level: INFO

Description: Failed creating an oauth 2.0 refresh token

Data: message, token info

Triggers: Failed creating an oauth 2.0 refresh token

CREATED_AUTHORIZATION_CODE

ID: OAuth2Provider-7

Level: INFO

Description: Created an oauth 2.0 authorization code

Data: message, token info

Triggers: Created an oauth 2.0 authorization code refresh token

FAILED_CREATE_AUTHORIZATION_CODE

ID: OAuth2Provider-8

Level: INFO

Description: Failed creating an oauth 2.0 authorization code

Data: message, token info

Triggers: Failed creating an oauth 2.0 authorization code

FAILED_UPDATE_AUTHORIZATION_CODE

ID: OAuth2Provider-9

Level: INFO

Description: Failed updating an oauth 2.0 authorization code

Data: message, token info

Triggers: Failed updating an oauth 2.0 authorization code

CREATED_CLIENT

ID: OAuth2Provider-11

Level: INFO

Description: Created an oauth 2.0 Client

Data: message, token info

Triggers: Created a new oauth 2.0 client

DELETED_CLIENT

ID: OAuth2Provider-12

Level: INFO

Description: Deleted an oauth 2.0 client

Data: message, token info

Triggers: Deleted an oauth 2.0 client

FAILED_CREATE_CLIENT

ID: OAuth2Provider-13

Level: INFO

Description: Failed to creating an oauth 2.0 client

Triggers: Failed creating an oauth 2.0 client

FAILED_DELETE_CLIENT

ID: OAuth2Provider-14

Level: INFO

Description: Failed deleting an oauth 2.0 client

Triggers: Failed deleting an oauth 2.0 client

AUTHENTICATED_CLIENT

ID: OAuth2Provider-15

Level: INFO

Description: Authenticated an oauth 2.0 client

Data: client id

Triggers: Authenticated an oauth 2.0 client

FAILED_AUTHENTICATE_CLIENT

ID: OAuth2Provider-16

Level: INFO

Description: Failed authenticating an oauth 2.0 client

Data: client id

Triggers: Failed authenticating an oauth 2.0 client

UPDATED_AUTHORIZATION_CODE

ID: OAuth2Provider-17

Level: INFO

Description: Updated an OAuth2 authorization code

Data: message, token info

Triggers: Updated an OAuth2 authorization code

OpenAM logs the following POLICY messages.

POLICY_EVALUATION

ID: POLICY-1

Level: INFO

Description: Evaluating policy succeeded

Data: policy name, realm name, service type name, resource name, action names, policy decision

Triggers: Evaluating policy.

PROTECTED_RESOURCES

ID: POLICY-2

Level: INFO

Description: Getting protected policy resources succeeded

Data: principal name, resource name, protecting policies

Triggers: Getting protected policy resources.

POLICY_CREATE_SUCCESS

ID: POLICY-3

Level: INFO

Description: Creating policy in a realm succeeded

Data: policy name, realm name

Triggers: Creating policy in a realm.

POLICY_MODIFY_SUCCESS

ID: POLICY-4

Level: INFO

Description: Modifying policy in a realm succeeded

Data: policy name, realm name

Triggers: Modifying policy in a realm.

POLICY_REMOVE_SUCCESS

ID: POLICY-5

Level: INFO

Description: Removing policy from a realm succeeded

Data: policy name, realm name

Triggers: Removing policy from a realm.

POLICY_ALREADY_EXISTS_IN_REALM

ID: POLICY-6

Level: INFO

Description: Policy already exists in the realm

Data: policy name, realm name

Triggers: Creating policy in the realm.

UNABLE_TO_ADD_POLICY

ID: POLICY-7

Level: INFO

Description: Creating policy in a realm failed

Data: policy name, realm name

Triggers: Creating policy in a realm.

Actions: Check if the user has privilege to create a policy in the realm.

UNABLE_TO_REPLACE_POLICY

ID: POLICY-8

Level: INFO

Description: Replacing policy in a realm failed

Data: policy name, realm name

Triggers: Replacing policy in a realm.

Actions: Check if the user has privilege to replace a policy in the realm.

DID_NOT_REPLACE_POLICY

ID: POLICY-81

Level: INFO

Description: Did not replace policy - A diifferent policy with the new name already exists in the realm

Data: new policy name, realm name

Triggers: Replacing policy in a realm

UNABLE_TO_REMOVE_POLICY

ID: POLICY-9

Level: INFO

Description: Removing policy from a realm failed

Data: policy name, realm name

Triggers: Removing policy from a realm.

Actions: Check if the user has privilege to remove a policy from the realm.

PROXIED_POLICY_EVALUATION

ID: POLICY-10

Level: INFO

Description: Computing policy decision by an administrator succeeded

Data: admin name, principal name, resource name, policy decision

Triggers: Computing policy decision by an administrator.

PROXIED_POLICY_EVALUATION_IGNORING_SUBJECTS

ID: POLICY-11

Level: INFO

Description: Computing policy decision by an administrator ignoring subjects succeeded

Data: admin name, resource name, policy decision

Triggers: Computing policy decision by an administrator ignoring subjects.

OpenAM logs the following Rest messages.

ATTEMPT_ACCESS

ID: Rest-1

Level: INFO

Description: Attempted to access a REST resource.

Data: resource, operation

Triggers: Attempting to access a REST resource.

ACCESS_GRANT

ID: Rest-2

Level: INFO

Description: Access granted to a REST resource.

Data: resource, operation, authzModule

Triggers: Access was granted to the requested resource.

ACCESS_DENY

ID: Rest-3

Level: INFO

Description: Access denied to a REST resource.

Data: resource, operation, authzModule

Triggers: Access was denied to the requested resource.

OpenAM logs the following SESSION messages.

SESSION_CREATED

ID: SESSION-1

Level: INFO

Description: Session is Created

Data: User ID

Triggers: User is authenticated.

SESSION_IDLE_TIMED_OUT

ID: SESSION-2

Level: INFO

Description: Session has idle timedout

Data: User ID

Triggers: User session idle for long time.

SESSION_MAX_TIMEOUT

ID: SESSION-3

Level: INFO

Description: Session has Expired

Data: User ID

Triggers: User session has reached its maximun time limit.

SESSION_LOGOUT

ID: SESSION-4

Level: INFO

Description: User has Logged out

Data: User ID

Triggers: User has logged out of the system.

SESSION_REACTIVATION

ID: SESSION-5

Level: INFO

Description: Session is Reactivated

Data: User ID

Triggers: User session state is active.

SESSION_DESTROYED

ID: SESSION-6

Level: INFO

Description: Session is Destroyed

Data: User ID

Triggers: User session is destroyed and cannot be referenced.

SESSION_PROPERTY_CHANGED

ID: SESSION-7

Level: INFO

Description: Session's property is changed.

Data: User ID

Triggers: User changed session's unprotected property.

SESSION_UNKNOWN_EVENT

ID: SESSION-8

Level: INFO

Description: Session received Unknown Event

Data: User ID

Triggers: Unknown session event

SESSION_PROTECTED_PROPERTY_ERROR

ID: SESSION-9

Level: INFO

Description: Attempt to set protected property

Data: User ID

Triggers: Attempt to set protected property

SESSION_QUOTA_EXHAUSTED

ID: SESSION-10

Level: INFO

Description: User's session quota has been exhausted.

Data: User ID

Triggers: Session quota exhausted

SESSION_DATABASE_UNAVAILABLE

ID: SESSION-11

Level: INFO

Description: Session database used for session failover and session constraint is not available.

Data: User ID

Triggers: Unable to reach the session database.

SESSION_DATABASE_BACK_ONLINE

ID: SESSION-12

Level: INFO

Description: Session database is back online.

Data: User ID

Triggers: Session database is back online..

SESSION_MAX_LIMIT_REACHED

ID: SESSION-13

Level: INFO

Description: The total number of valid sessions hosted on the AM server has reached the max limit.

Data: User ID

Triggers: Session max limit reached.

Glossary

Access control	Control to grant or to deny access to a resource.
Account lockout	The act of making an account temporarily or permanently inactive after successive authentication failures.
Actions	Defined as part of policies, these verbs indicate what authorized identities can do to resources.
Advice	In the context of a policy decision denying access, a hint to the policy enforcement point about remedial action to take that could result in a decision allowing access.
Agent administrator	User having privileges only to read and write agent profile configuration information, typically created to delegate agent profile creation to the user installing a web or Java agent.
Agent authenticator	Entity with read-only access to multiple agent profiles defined in the same realm; allows an agent to read web service profiles.
Application	In general terms, a service exposing protected resources. In the context of AM policies, the application is a template that constrains the policies that govern access to protected resources. An application can have zero or more policies.
Application type	Application types act as templates for creating policy applications. Application types define a preset list of actions and functional logic, such as policy lookup and resource comparator logic.

	Application types also define the internal normalization, indexing logic, and comparator logic for applications.
Attribute-based access control (ABAC)	Access control that is based on attributes of a user, such as how old a user is or whether the user is a paying customer.
Authentication	The act of confirming the identity of a principal.
Authentication chaining	A series of authentication modules configured together which a principal must negotiate as configured in order to authenticate successfully.
Authentication level	Positive integer associated with an authentication module, usually used to require success with more stringent authentication measures when requesting resources requiring special protection.
Authentication module	AM authentication unit that handles one way of obtaining and verifying credentials.
Authorization	The act of determining whether to grant or to deny a principal access to a resource.
Authorization Server	In OAuth 2.0, issues access tokens to the client after authenticating a resource owner and confirming that the owner authorizes the client to access the protected resource. AM can play this role in the OAuth 2.0 authorization framework.
Auto-federation	Arrangement to federate a principal's identity automatically based on a common attribute value shared across the principal's profiles at different providers.
Bulk federation	Batch job permanently federating user profiles between a service provider and an identity provider based on a list of matched user identifiers that exist on both providers.
Circle of trust	Group of providers, including at least one identity provider, who have agreed to trust each other to participate in a SAML v2.0 provider federation.
Client	In OAuth 2.0, requests protected web resources on behalf of the resource owner given the owner's authorization. AM can play this role in the OAuth 2.0 authorization framework.
Client-based OAuth 2.0 tokens	After a successful OAuth 2.0 grant flow, AM returns a token to the client. This differs from CTS-based OAuth 2.0 tokens, where AM returns a *reference* to token to the client.
Client-based sessions	AM sessions for which AM returns session state to the client after each request, and require it to be passed in with the subsequent

	request. For browser-based clients, AM sets a cookie in the browser that contains the session information. For browser-based clients, AM sets a cookie in the browser that contains the session state. When the browser transmits the cookie back to AM, AM decodes the session state from the cookie.
Conditions	Defined as part of policies, these determine the circumstances under which which a policy applies. Environmental conditions reflect circumstances like the client IP address, time of day, how the subject authenticated, or the authentication level achieved. Subject conditions reflect characteristics of the subject like whether the subject authenticated, the identity of the subject, or claims in the subject's JWT.
Configuration datastore	LDAP directory service holding AM configuration data.
Cross-domain single sign-on (CDSSO)	AM capability allowing single sign-on across different DNS domains.
CTS-based OAuth 2.0 tokens	After a successful OAuth 2.0 grant flow, AM returns a *reference* to the token to the client, rather than the token itself. This differs from client-based OAuth 2.0 tokens, where AM returns the entire token to the client.
CTS-based sessions	AM sessions that reside in the Core Token Service's token store. CTS-based sessions might also be cached in memory on one or more AM servers. AM tracks these sessions in order to handle events like logout and timeout, to permit session constraints, and to notify applications involved in SSO when a session ends.
Delegation	Granting users administrative privileges with AM.
Entitlement	Decision that defines which resource names can and cannot be accessed for a given identity in the context of a particular application, which actions are allowed and which are denied, and any related advice and attributes.
Extended metadata	Federation configuration information specific to AM.
Extensible Access Control Markup Language (XACML)	Standard, XML-based access control policy language, including a processing model for making authorization decisions based on policies.
Federation	Standardized means for aggregating identities, sharing authentication and authorization data information between trusted providers, and

	allowing principals to access services across different providers without authenticating repeatedly.
Fedlet	Service provider application capable of participating in a circle of trust and allowing federation without installing all of AM on the service provider side; AM lets you create Java Fedlets.
Hot swappable	Refers to configuration properties for which changes can take effect without restarting the container where AM runs.
Identity	Set of data that uniquely describes a person or a thing such as a device or an application.
Identity federation	Linking of a principal's identity across multiple providers.
Identity provider (IDP)	Entity that produces assertions about a principal (such as how and when a principal authenticated, or that the principal's profile has a specified attribute value).
Identity repository	Data store holding user profiles and group information; different identity repositories can be defined for different realms.
Java agent	Java web application installed in a web container that acts as a policy enforcement point, filtering requests to other applications in the container with policies based on application resource URLs.
Metadata	Federation configuration information for a provider.
Policy	Set of rules that define who is granted access to a protected resource when, how, and under what conditions.
Policy agent	Java, web, or custom agent that intercepts requests for resources, directs principals to AM for authentication, and enforces policy decisions from AM.
Policy Administration Point (PAP)	Entity that manages and stores policy definitions.
Policy Decision Point (PDP)	Entity that evaluates access rights and then issues authorization decisions.
Policy Enforcement Point (PEP)	Entity that intercepts a request for a resource and then enforces policy decisions from a PDP.
Policy Information Point (PIP)	Entity that provides extra information, such as user profile attributes that a PDP needs in order to make a decision.
Principal	Represents an entity that has been authenticated (such as a user, a device, or an application), and thus is distinguished from other entities.

	When a Subject successfully authenticates, AM associates the Subject with the Principal.
Privilege	In the context of delegated administration, a set of administrative tasks that can be performed by specified identities in a given realm.
Provider federation	Agreement among providers to participate in a circle of trust.
Realm	AM unit for organizing configuration and identity information. Realms can be used for example when different parts of an organization have different applications and identity stores, and when different organizations use the same AM deployment. Administrators can delegate realm administration. The administrator assigns administrative privileges to users, allowing them to perform administrative tasks within the realm.
Resource	Something a user can access over the network such as a web page. Defined as part of policies, these can include wildcards in order to match multiple actual resources.
Resource owner	In OAuth 2.0, entity who can authorize access to protected web resources, such as an end user.
Resource server	In OAuth 2.0, server hosting protected web resources, capable of handling access tokens to respond to requests for such resources.
Response attributes	Defined as part of policies, these allow AM to return additional information in the form of "attributes" with the response to a policy decision.
Role based access control (RBAC)	Access control that is based on whether a user has been granted a set of permissions (a role).
Security Assertion Markup Language (SAML)	Standard, XML-based language for exchanging authentication and authorization data between identity providers and service providers.
Service provider (SP)	Entity that consumes assertions about a principal (and provides a service that the principal is trying to access).
Authentication Session	The interval while the user or entity is authenticating to AM.
Session	The interval that starts after the user has authenticated and ends when the user logs out, or when their session is terminated. For browser-based clients, AM manages user sessions across one or more applications by setting a session cookie. See also CTS-based sessions and Client-based sessions.

Session high availability	Capability that lets any AM server in a clustered deployment access shared, persistent information about users' sessions from the CTS token store. The user does not need to log in again unless the entire deployment goes down.
Session token	Unique identifier issued by AM after successful authentication. For a CTS-based sessions, the session token is used to track a principal's session.
Single log out (SLO)	Capability allowing a principal to end a session once, thereby ending her session across multiple applications.
Single sign-on (SSO)	Capability allowing a principal to authenticate once and gain access to multiple applications without authenticating again.
Site	Group of AM servers configured the same way, accessed through a load balancer layer. The load balancer handles failover to provide service-level availability. The load balancer can also be used to protect AM services.
Standard metadata	Standard federation configuration information that you can share with other access management software.
Stateless Service	Stateless services do not store any data locally to the service. When the service requires data to perform any action, it requests it from a data store. For example, a stateless authentication service stores session state for logged-in users in a database. This way, any server in the deployment can recover the session from the database and service requests for any user. All AM services are stateless unless otherwise specified. See also Client-based sessions and CTS-based sessions.
Subject	Entity that requests access to a resource When an identity successfully authenticates, AM associates the identity with the Principal that distinguishes it from other identities. An identity can be associated with multiple principals.
Identity store	Data storage service holding principals' profiles; underlying storage can be an LDAP directory service or a custom `IdRepo` implementation.
Web Agent	Native library installed in a web server that acts as a policy enforcement point with policies based on web page URLs.