

Properties reference

This reference covers agent configuration properties.

When you create the agent profile, you choose whether to store the agent configuration in AM's configuration store or locally to the agent installation. The local configuration file syntax is the same as of a standard Java properties file.

Property aliases

A property alias specifies a path for a property. One property can have an unlimited number of aliases, however, an alias must be unique.

How the agent manages multiple aliases

When a property has multiple aliases, the agent evaluates the aliases in alphabetical order. If each alias specifies a different value for the property, the agent assigns the value specified by the first alias in the alphabetical order, and then propagates that value to the other aliases.

The following example assigns different values to a property with three aliases:

```
com.sun.identity.agents.app.username=AGENT3  
com.sun.identity.agents.config.profilename=AGENT1  
org.forgerock.agents.profile.name=AGENT2
```

The agent evaluates `com.sun.identity.agents.app.username` first, and propagates that value to the other aliases, resulting in this:

```
com.sun.identity.agents.app.username=AGENT3  
com.sun.identity.agents.config.profilename=AGENT3  
org.forgerock.agents.profile.name=AGENT3
```

How AM manages multiple aliases

Each version of AM recognizes a different group of agent aliases. When you are using AM commands, such as `ssoadm` to configure an agent, consider the following points on using recognized and unrecognized aliases:

- When you use a recognized alias in an `ssoadm` command (for example, `com.sun.identity.agents.config.notenforced.ip.cache.size=2000`), the agent updates the value for the property represented by that alias.

For the above example, **Max Entries in Not-Enforced IP Cache** is displayed as `2000` in the **Application** tab of the AM console.

- When you use an unrecognized alias in an `ssoadm` command (for example, `org.forgerock.agents.config.notenforced.ip.cache.size=4000`), the agent creates a custom property.

For the above example, `org.forgerock.agents.config.notenforced.ip.cache.size=4000` is displayed in **Custom Properties**, in the **Advanced** tab of the AM console.

- When a property is set by both a standard property and a custom property, the custom property takes precedence. The value of the standard property is not updated, and both values are displayed in the configuration.

Property files

The agent searches for local property files in a location defined by a property added to `JAVA_OPTS`.

In Tomcat, the agent can take the file location from `bin/setenv.sh` as follows:

```
JAVA_OPTS="$JAVA_OPTS -
Dopenam.agents.bootstrap.dir=/path/to/agents/agent/agent_instance
/config"
```

Bootstrap properties

The agent configurations support the following bootstrap properties:

- [Agent Filter Mode Map](#)
- [Agent Profile Name](#)
- [Agent Profile Realm](#)
- [AM Authentication Service Host Name](#)
- [AM Authentication Service Path](#)
- [AM Authentication Service Port](#)
- [AM Authentication Service Protocol](#)
- [Autonomous mode](#)
- [CSV Monitoring Directory](#)
- [Enable Configuration Lock](#)

- [Enable HTTP Connection Reuse](#)
- [Enable HTTP Connection State](#)
- [Enable HTTP Retry](#)
- [Enable Notification of Policy Changes](#)
- [Enable Notifications of Agent Configuration Change](#)
- [Enable Prometheus Monitoring](#)
- [Encryption Class](#)
- [Exchanged SSO Token Cache TTL](#)
- [Expired Session Cache Timeout](#)
- [HTTP Connection Timeout](#)
- [HTTP Socket Timeout](#)
- [Java Class for Matching Not Enforced Rules](#)
- [JWT Cache TTL](#)
- [JWT Cookie Name](#)
- [Local Audit Log Filename](#)
- [Location of Agent Configuration Repository](#)
- [Max Entries in Expired Session Cache](#)
- [Max Entries in JWT Cache](#)
- [Max Entries in Policy Cache per Session](#)
- [Max Entries in POST Data Preservation Storage](#)
- [Max Entries in SSO Exchange Cache](#)
- [Max HTTP Connection Count](#)
- [Max Sessions in Policy Cache](#)
- [Not-Enforced Favicon](#)
- [Policy Cache TTL](#)
- [POST Data Preservation Cache TTL](#)
- [POST Data Preservation Cache TTL in Milliseconds \(deprecated\)](#)
- [POST Data Preservation Directory Sweep Interval](#)
- [POST Data Preservation Storage Size](#)
- [Public AM URL](#)
- [Service Resolver Class Name](#)
- [Session Cache TTL](#)
- [Strategy when AM unavailable](#)

Properties by function

The agent configurations support properties that have the following functions.

Access denied

- [Access Denied URI Map](#)

Agent

- [Alternative Agent Protocol](#)
- [Autonomous mode](#)
- [Recheck availability of AM](#)
- [Alternative Agent Port Number](#)
- [Alternative Agent Host Name](#)
- [Agent Filter Mode Map](#)
- [Strategy when AM unavailable](#)

Attributes

- [Session Attribute Fetch Mode](#)
- [Cookie Separator Character](#)
- [Fetch Attribute Date Format](#)
- [Response Attribute Fetch Mode](#)
- [Profile Attribute Fetch Mode](#)
- [Enable Attribute Encoding](#)

Audit

- [Enable Local Audit Log Rotation](#)
- [Local Audit Log Rotation Size](#)
- [Audit Logfile Retention Count](#)
- [Audit Access Types](#)
- [Local Audit Log Filename](#)
- [Audit Log Location](#)

Authentication failure

- [Authentication Fail Reason Parameter Name](#)
- [Authentication Fail Reason Parameter Value Map](#)
- [Authentication Fail URL](#)
- [Goto URL](#)

Authentication service

- [AM Authentication Service Path](#)
- [AM Authentication Service Protocol](#)
- [Encryption Key/Salt](#)
- [AM Authentication Service Host Name](#)
- [AM Authentication Service Port](#)

Client identification

- [Client Hostname Header](#)
- [Client IP Validation Mode](#)
- [Client IP Validation Address Map](#)
- [Client IP Address Header](#)

Connection pooling

- [Max HTTP Connection Count](#)
- [HTTP Connection Timeout](#)
- [Enable HTTP Connection Reuse](#)
- [Enable HTTP Connection State](#)
- [Enable Connection Pooling](#)
- [HTTP Socket Timeout](#)
- [Enable HTTP Retry](#)

Container

- [Container Character Encoding](#)
- [Container Parameter Encoding](#)

Continuous security

- [Continuous Security Cookie Map](#)

- [Continuous Security Header Map](#)
- [Client Hostname Header](#)
- [Client IP Address Header](#)

Cookie

- [Maximum Decompression Size](#)
- [Pre-Authn and Post Data Preservation Cookie Signing Value](#)
- [Max Age of Pre-Authentication Cookie](#)
- [Load Balancer Cookie Name](#)
- [Enable Encoded Cookies](#)
- [Enable HTTP Only Cookies](#)
- [Pre-Authentication Cookie Name](#)
- [Post Data Preservation Cookie Name](#)
- [Enable Load Balancer Cookies](#)

Cookie reset

- [Reset Cookie List](#)
- [Session Attribute Fetch Mode](#)
- [Cookie Reset](#)
- [Reset Cookie Domain Map](#)
- [Reset Cookie Path Map](#)
- [Profile Attribute Fetch Mode](#)

Cross-domain single sign-on

- [Transmit Cookies Securely](#)
- [Authentication Redirect URI](#)

Cross-site scripting

- [XSS Code Element List](#)
- [XSS Redirect URI Map](#)

Custom login redirect

- [Enable SSO Token Acceptance](#)

- [OAuth Login URL List](#)
- [Enable Custom Login Mode](#)
- [AM Login URL List](#)
- [Login Reason Parameter Name](#)
- [Legacy Login URL List](#)

Default Login Redirect

- [OAuth Login URL List](#)
- [Enable Custom Login Mode](#)
- [AM Login URL List](#)
- [Legacy Login URL List](#)

Deprecated

- [Debug File Rotation Size \(deprecated\)](#)
- [Log File Directory \(deprecated\)](#)
- [Debug File Rotation Suffix \(deprecated\)](#)
- [Debug File Rotation Retention Count \(deprecated\)](#)
- [Debug File Rotation Time \(deprecated\)](#)
- [Debug File Rotation Prefix \(deprecated\)](#)

Encryption

- [Encryption Class](#)
- [Encryption Key/Salt](#)

Fragment

- [Fragment Relay URL](#)

Fully qualified domain name

- [Default FQDN](#)
- [FQDN Map](#)
- [Enable FQDN Checking](#)

Global

- [Enable Prometheus Monitoring](#)
- [HTTP 302 Redirect Data](#)
- [HTTP 302 Redirect Not-Enforced List](#)
- [HTTP 302 Redirect Replacement HTTP Status Code](#)
- [Goto Parameter Name](#)
- [HTTP 302 Redirect Content Type](#)
- [HTTP 302 Redirect Invert Not-Enforced List](#)
- [Enable HTTP 302 Redirects](#)

Legacy support

- [Enable Legacy Support Handlers \(deprecated\)](#)
- [Legacy User Agent Redirect URL \(deprecated\)](#)
- [Legacy User Agent List \(deprecated\)](#)

Locale

- [Locale Country](#)
- [Locale Language](#)

Login

- [Enable Redirect to AM Success URL](#)
- [Login Attempt Limit](#)
- [Authentication Exchange Cookie Name](#)
- [Login Attempt Limit Cookie Name](#)
- [Login Reason Value Map](#)
- [Redirect Attempt Limit](#)
- [Authentication Exchange URI](#)

Login Redirect (Default)

- [OAuth Login URL List](#)
- [Enable Custom Login Mode](#)
- [AM Login URL List](#)
- [Legacy Login URL List](#)

Login redirect

- [Enable SSO Token Acceptance](#)
- [OAuth Login URL List](#)
- [Enable Custom Login Mode](#)
- [AM Login URL List](#)
- [Login Reason Parameter Name](#)
- [Legacy Login URL List](#)

Logout

- [Logout URI Map](#)
- [Logout Request Parameter Map](#)
- [Always invalidate sessions](#)
- [Enable Logout Introspection](#)
- [Conditional Logout URL List](#)
- [Logout Entry URI Map](#)

Logs

- [Agent Debug Level](#)

Miscellaneous

- [Redirect Attempt Cookie Name](#)
- [Encrypted Agent Password](#)
- [Enable Ignore Path Info](#)
- [Custom Response Header Map](#)
- [Idle Time Refresh Window](#)
- [Service Resolver Class Name](#)
- [HTTP Session Binding](#)
- [Public AM URL](#)

Monitoring

- [Export Monitoring Metrics to CSV](#)
- [CSV Monitoring Directory](#)

Not-enforced

- [Not-Enforced URIs](#)
- [Not-Enforced Client IP List](#)
- [Not-Enforced Favicon](#)
- [Enable Not-Enforced URIs Cache](#)
- [Container Character Encoding](#)
- [Java Class for Matching Not Enforced Rules](#)
- [Not-Enforced Compound Rule Separator](#)
- [Invert Not-Enforced URIs](#)
- [Max Entries in Not-Enforced URI Cache](#)
- [Enable Not-Enforced IP Cache](#)
- [Invert Not-Enforced IPs](#)
- [Max Entries in Not-Enforced IP Cache](#)
- [Container Parameter Encoding](#)

Notifications

- [Enable Notifications of Agent Configuration Change](#)
- [Obsolete Notification URL \(deprecated\)](#)
- [Enable Notification of Session Logout \(deprecated\)](#)
- [Enable Notification of Policy Changes](#)
- [Enable Notification of Session Logout](#)

POST data preservation

- [POST Data Preservation Directory Sweep Interval](#)
- [Missing POST Data Preservation Entry URI Map](#)
- [POST Data Preservation Cache TTL](#)
- [POST Data Preservation Sticky Session Key Value](#)
- [POST Data Preservation Sticky Session Mode](#)
- [Enable POST Data Preservation](#)
- [POST Data Preservation in Files or Cache](#)
- [Pre-Authn and Post Data Preservation Cookie Signing Value](#)
- [POST Data Preservation Storage Size](#)

- [Max Entries in POST Data Preservation Storage](#)
- [POST Data Preservation File Directory](#)
- [Post Data Preservation Cookie Name](#)
- [POST Data Preservation Cache TTL in Milliseconds \(deprecated\)](#)

Policy enforcement

- [POST Parameter List for URL Policy Env](#)
- [Max Entries in Policy Cache per Session](#)
- [Restrict to Realm Map](#)
- [Enable Composite Advice Encoding](#)
- [Max Sessions in Policy Cache](#)
- [Enable Policy Evaluation in User Authentication Realm](#)
- [GET Parameter List for URL Policy Env](#)
- [Policy Cache TTL](#)
- [JSession Parameter List for URL Policy Env](#)
- [Policy Evaluation Realm Map](#)
- [Policy Set Map](#)

Port check

- [Port Check Filename \(deprecated\)](#)
- [Port Check Protocol Map \(deprecated\)](#)
- [Enable Port Checking \(deprecated\)](#)

Pre-authentication

- [Pre-Authn and Post Data Preservation Cookie Signing Value](#)
- [Max Age of Pre-Authentication Cookie](#)
- [Pre-Authentication Cookie Name](#)

Profile

- [Fall-Forward Mode \(deprecated\)](#)
- [Location of Agent Configuration Repository](#)
- [JWT Cookie Domain List](#)
- [JWT Cache TTL](#)

- [Max Entries in JWT Cache](#)
- [JWT Cookie Name](#)
- [Agent Profile Realm](#)
- [Exchanged SSO Token Cache TTL](#)
- [Configuration Reload Interval](#)
- [Agent Profile Name](#)
- [Enable Configuration Lock](#)
- [Profile Attribute Map](#)
- [Max Entries in SSO Exchange Cache](#)
- [Profile Attribute Fetch Mode](#)
- [WebSocket Connection Interval](#)

Query parameter

- [Regex Remove Query Parameters List for Policy Evaluation](#)
- [Remove Query Parameters List for Policy Evaluation](#)
- [Regex Query Parameters List for Policy Evaluation](#)
- [Query Parameter List for Policy Evaluation](#)

Required

- [AM Authentication Service Path](#)
- [Authentication Redirect URI](#)
- [Encryption Class](#)
- [AM Authentication Service Protocol](#)
- [Agent Profile Realm](#)
- [Encrypted Agent Password](#)
- [Location of Agent Configuration Repository](#)
- [Agent Profile Name](#)
- [Autonomous mode](#)
- [AM Authentication Service Host Name](#)
- [AM Authentication Service Port](#)
- [Public AM URL](#)

Response

- [Response Attribute Map](#)
- [Response Attribute Fetch Mode](#)

SSO cookie handling

- [Enable SSO Token Acceptance](#)
- [Convert SSO Tokens Into OIDC JWTs](#)
- [SSO Cookie Domain List](#)

SameSite

- [Set-Cookie Internal Map](#)
- [Exclude Agents From Samesite Cookie Attributes](#)
- [Set-Cookie Attribute Map](#)

Session

- [Session Attribute Fetch Mode](#)
- [Session Attribute Map](#)
- [Session Cache TTL](#)
- [Max Entries in Expired Session Cache](#)
- [Expired Session Cache Timeout](#)

Timeout

- [Websocket Idle Timeout](#)
- [Websocket Expired Timeout](#)

User mapping

- [User Attribute Name](#)
- [User Mapping Mode](#)
- [User Session Name](#)
- [Enable User Principal Flag](#)

Access denied

Access Denied URI Map

The URIs of custom pages to return when access is denied. The key is the web application name. The value is the custom URI.

To set a global custom access denied URI for web applications without other custom access denied URIs defined, leave the key empty and set the value to the global custom access denied URI, `/sample/accessdenied.html`.

To set a custom access denied URI for a specific web application, set the key to the name of the web application, and the value to the web application access denied URI, such as `/myApp/accessdenied.html`.

Specify a full URL if required, including the host name. For example:
`https://help.example.com/errors/accessdenied.html`.

Property name	<code>org.forgerock.agents.access.denied.uri.map</code>
Aliases	<code>com.sun.identity.agents.config.access.denied.uri</code> Introduced in Java Agent 5.0 <u>Recognized</u> from AM 6 <code>org.forgerock.agents.access.denied.uri.map</code> Introduced in Java Agent 5.6
Type	Map <ul style="list-style-type: none">• Keys: web application• Values: URI of page saying 'access denied'
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>
AM console	Tab: Application Title: Access Denied URI Map Legacy title: Resource Access Denied URI

Agent

Alternative Agent Protocol

In environments when agents are behind a load balancer or reverse proxy which does a SSL offloading, the request URL is changed to match the URL that the agent receives.

The agent then uses the new URL as the redirection value in the pre-authentication cookie, created during the first unauthenticated request to the agent.

Use the following properties to override the agent redirection value with the URL of the original client request: [Alternative Agent Host Name](#), and [Alternative Agent Port Number](#).

Property name	<code>org.forgerock.agents.agent.protocol</code>
Aliases	<code>com.sun.identity.agents.config.agent.protocol</code> Introduced in Java Agent 5.0 <u>Recognized</u> from AM 6 <code>org.forgerock.agents.agent.protocol</code> Introduced in Java Agent 5.6
Type	String
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>
AM console	Tab: Advanced Title: Alternative Agent Protocol

Autonomous mode

When `true` the agent operates independently of AM, without needing to contact an AM instance. Agents allow access to resources as defined in not-enforced lists; otherwise, they deny access.

Property name	<code>org.forgerock.agents.fallback.mode.enabled</code>
---------------	---

Aliases	<code>com.forgerock.agents.config.fallback.mode</code> Introduced in Java Agent 5.9.0 <code>org.forgerock.agents.fallback.mode.enabled</code> Introduced in Java Agent 5.9.0 <code>org.forgerock.agents.autonomous.mode.enabled</code> Introduced in Java Agent 5.9.0
Type	Boolean: <code>true</code> returns true; all other strings return <code>false</code> .
Default	<code>false</code>
Bootstrap property	Yes
Required property	Yes - If this property is missing, the agent fails to start
Restart required	Yes - Restart the container after changing the property
Local configuration file	<code>AgentBootstrap.properties</code>

Recheck availability of AM

The duration after which the agent rechecks AM availability, when Autonomous mode is `false`, and AM becomes unavailable at runtime.

Consider these points when you configure this property:

- If the duration is too short, the agent checks AM availability too often, and agent performance can be reduced.
- If the duration is zero, the agent checks AM availability for every call. Requests that match not-enforced rules can take longer.

Property name	<code>org.forgerock.agents.am.unavailability.recheck.window.in.seconds</code>
Aliases	<code>org.forgerock.agents.am.unavailability.recheck.window.in.seconds</code> Introduced in Java Agent 5.9.0 <u>Recognized</u> from AM 7.2
Type	Integer
Default	5

Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	AgentConfig.properties
AM console	Tab: Profile (from AM 7.2) Title: Recheck availability of AM

Alternative Agent Port Number

In environments when agents are behind a load balancer or reverse proxy which does a SSL offloading, the request URL is changed to match the URL that the agent receives.

The agent then uses the new URL as the redirection value in the pre-authentication cookie, created during the first unauthenticated request to the agent.

Use the following properties to override the agent redirection value with the URL of the original client request: [Alternative Agent Host Name](#), and [Alternative Agent Protocol](#).

Property name	org.forgerock.agents.agent.port
Aliases	com.sun.identity.agents.config.agent.port Introduced in Java Agent 5.0 Recognized from AM 6 org.forgerock.agents.agent.port Introduced in Java Agent 5.6
Type	Integer
Default	-2147483648
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	AgentConfig.properties
AM console	Tab: Advanced Title: Alternative Agent Port Number

Alternative Agent Host Name

In environments when agents are behind a load balancer or reverse proxy which does a SSL offloading, the request URL is changed to match the URL that the agent receives.

The agent then uses the new URL as the redirection value in the pre-authentication cookie, created during the first unauthenticated request to the agent.

Use the following properties to override the agent redirection value with the URL of the original client request: [Alternative Agent Port Number](#) and [Alternative Agent Protocol](#).

Property name	<code>org.forgerock.agents.agent.hostname</code>
Aliases	<code>com.sun.identity.agents.config.agent.host</code> Introduced in Java Agent 5.0 <u>Recognized</u> from AM 6 <code>org.forgerock.agents.agent.hostname</code> Introduced in Java Agent 5.6
Type	String
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>
AM console	Tab: Advanced Title: Alternative Agent Host Name

Agent Filter Mode Map

A map of web application name to agent filter mode:

- Key: Web application name.
- Value: Agent filter mode.

The following example configures one filter mode for the `BankApp` web application. All other web applications use the default filter mode, `URL_POLICY` :

```
org.forgerock.agents.filter.mode.map[BankApp]=SSO_ONLY
```

The following example configures the `NONE` filter mode for all applications in the web container: `org.forgerock.agents.filter.mode.map[ALL]=NONE`

The mode `J2EE_POLICY` does not apply to Java Agents 5.10. However, for backward-compatibility, it is displayed in the AM agent profile page.

Property name	<code>org.forgerock.agents.filter.mode.map</code>
Aliases	<p><code>com.sun.identity.agents.config.filter.mode</code> Introduced in Java Agent 5.0 <u>Recognized</u> from AM 6</p> <p><code>org.forgerock.agents.filter.mode.map</code> Introduced in Java Agent 5.6.2.1</p>
Supported settings	<p><i>NONE</i> The agent performs no authentication check, and grants access to any resource. When the value is <code>NONE</code> and logging is enabled, for auditing purposes, the agent filter logs all incoming requests.</p> <p><i>SSO_ONLY</i> Any user having either a valid SSO token or JWT can access any resource.</p> <p><i>URL_POLICY</i> The normal operating mode of the agent, in which resource access is granted by AM policy evaluation.</p>
Default	<code>URL_POLICY</code>
Bootstrap property	Yes
Required property	No
Restart required	No
Local configuration file	<code>AgentBootstrap.properties</code>
AM console	<p>Tab: Global</p> <p>Title: Agent Filter Mode Map</p> <p>Legacy title: Agent Filter Mode</p>

Strategy when AM unavailable

When Autonomous mode is `false`, this property defines the strategy to use when AM becomes unavailable at runtime (for example, due to network errors).

Property name	<code>org.forgerock.agents.strategy.when.am.unavailable</code>
Aliases	<code>org.forgerock.agents.strategy.when.am.unavailable</code> Introduced in Java Agent 5.9.0

Supported settings

IMMEDIATE_403

When AM is unavailable, every request immediately returns an HTTP 403

IMMEDIATE_503

When AM is unavailable, every request immediately return an HTTP 503

EVAL_NER_ELSE_403

When AM is unavailable, incoming requests are matched against not-enforced rules. Access is granted to matched resources, everything else returns HTTP 403.

EVAL_NER_ELSE_503

When AM is unavailable, incoming requests are matched against not-enforced rules. Access is granted to matched resources, everything else returns HTTP 503.

EVAL_NER_USE_CACHE_UNTIL_EXPIRED_ELSE_403

When AM is unavailable, incoming requests are matched against not-enforced rules. Unmatched requests are resolved against the cache. Requests unmatched by the cache result in HTTP 403. Cached entries expire naturally. Note that after the interval defined in "Policy Cache TTL" (org.forgerock.agents.policy.cache.ttl.minutes), this becomes exactly like EVAL_NER_ELSE_403.

EVAL_NER_USE_CACHE_UNTIL_EXPIRED_ELSE_503

When AM is unavailable, incoming requests are matched against not-enforced rules. Unmatched requests are resolved against the cache. Requests unmatched by the cache result in HTTP 503. Cached entries expire naturally. Note that after the interval defined in "Policy Cache TTL" (org.forgerock.agents.policy.cache.ttl.minutes), this becomes exactly like EVAL_NER_ELSE_503.

EVAL_NER_CACHE_INDEFINITELY_ELSE_403

As soon as AM becomes unavailable, values in the agent caches are frozen and preserved indefinitely. Incoming requests are matched against not-enforced rules. Unmatched requests are resolved against the

	<p>agent's frozen cache. Requests not matching the cache result in HTTP 403.</p> <p><i>EVAL_NER_CACHE_INDEFINITELY_ELSE_503</i></p> <p>As soon as AM becomes unavailable, values in the agent caches are frozen and preserved indefinitely. Incoming requests are matched against not-enforced rules. Unmatched requests are resolved against the agent's frozen cache. Requests not matching the cache result in HTTP 503.</p>
Default	EVAL_NER_USE_CACHE_UNTIL_EXPIRED_ELSE_503
Bootstrap property	Yes
Required property	No
Restart required	No
Local configuration file	AgentBootstrap.properties

Attributes

Session Attribute Fetch Mode

Map the name of an AM session attribute specified in [Session Attribute Map](#) as follows:

- NONE: Do not map
- HTTP_HEADER: Map the to the name of an HTTP session header
- HTTP_COOKIE: Map to the name of an HTTP cookie
- REQUEST_ATTRIBUTE: Map to the name of an HTTP session attribute

When the value is HTTP_COOKIE , [Cookie Reset](#) is automatically set to true . Before redirecting the client for login, and when the client logs out, the agent resets profile and session attributes cookies, and cookies in the [Reset Cookie List](#).

Property name	org.forgerock.agents.session.attribute.fetch.mode
---------------	---

Aliases	<p><code>org.forgerock.agents.session.attribute.fetch.mode</code></p> <p>Introduced in Java Agent 5.6</p> <p><code>com.sun.identity.agents.config.session.attribute.fetch.mode</code></p> <p>Introduced in Java Agent 5.0</p> <p><u>Recognized</u> from AM 6</p>
Supported settings	<p>NONE</p> <p>No AM attributes are mapped.</p> <p>HTTP_HEADER</p> <p>The named AM attributes are mapped to headers in the outgoing HTTP response.</p> <p>REQUEST_ATTRIBUTE</p> <p>The named AM attributes are mapped to request attributes in the outgoing HTTP response.</p> <p>HTTP_COOKIE</p> <p>The named AM attributes are mapped to cookies in the outgoing HTTP response.</p>
Default	NONE
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>
AM console	<p>Tab: Application</p> <p>Title: Session Attribute Fetch Mode</p>

Cookie Separator Character

The separator for multiple values of the same attribute when it is set as a cookie.

Property name	<code>org.forgerock.agents.attribute.cookie.separator</code>
---------------	--

Aliases	<p><code>com.sun.identity.agents.config.attribute.cookie.separator</code></p> <p>Introduced in Java Agent 5.0 <u>Recognized</u> from AM 6</p> <p><code>org.forgerock.agents.attribute.cookie.separator</code> Introduced in Java Agent 5.6</p>
Type	String
Default	
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>
AM console	<p>Tab: Application</p> <p>Title: Cookie Separator Character</p>

Fetch Attribute Date Format

The `java.text.SimpleDateFormat` of date attribute values used when an attribute is set in an HTTP header.

Property name	<code>org.forgerock.agents.attribute.date.format</code>
Aliases	<p><code>com.sun.identity.agents.config.attribute.date.format</code></p> <p>Introduced in Java Agent 5.0 <u>Recognized</u> from AM 6</p> <p><code>org.forgerock.agents.attribute.date.format</code> Introduced in Java Agent 5.6</p>
Type	String
Default	<code>EEE, d MMM yyyy hh:mm:ss z</code>
Bootstrap property	No
Required property	No

Restart required	No
Local configuration file	AgentConfig.properties
AM console	Tab: Application Title: Fetch Attribute Date Format

Response Attribute Fetch Mode

Map the name of an AM policy response attribute specified in [Response Attribute Map](#) as follows:

- NONE: Do not map
- HTTP_HEADER: Map the to the name of an HTTP response header
- HTTP_COOKIE: Map to the name of an HTTP cookie
- REQUEST_ATTRIBUTE: Map to the name of an HTTP request attribute

Property name	org.forgerock.agents.response.attribute.fetch.mode
Aliases	com.sun.identity.agents.config.response.attribute.fetch.mode Introduced in Java Agent 5.0 Recognized from AM 6 org.forgerock.agents.response.attribute.fetch.mode Introduced in Java Agent 5.6
Supported settings	NONE No AM attributes are mapped. HTTP_HEADER The named AM attributes are mapped to headers in the outgoing HTTP response. REQUEST_ATTRIBUTE The named AM attributes are mapped to request attributes in the outgoing HTTP response. HTTP_COOKIE The named AM attributes are mapped to cookies in the outgoing HTTP response.

Default	NONE
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	AgentConfig.properties
AM console	Tab: Application Title: Response Attribute Fetch Mode

Profile Attribute Fetch Mode

Map the name of an AM profile attribute specified in [Profile Attribute Map](#) as follows:

- NONE: Do not map
- HTTP_HEADER: Map the to the name of an HTTP profile header
- HTTP_COOKIE: Map to the name of an HTTP cookie
- REQUEST_ATTRIBUTE: Map to the name of an HTTP profile attribute

Property name	<code>org.forgerock.agents.profile.attribute.fetch.mode</code>
Aliases	<code>com.sun.identity.agents.config.profile.attribute.fetch.mode</code> Introduced in Java Agent 5.0 <u>Recognized</u> from AM 6 <code>org.forgerock.agents.profile.attribute.fetch.mode</code> Introduced in Java Agent 5.6

Supported settings	<p>NONE No AM attributes are mapped.</p> <p>HTTP_HEADER The named AM attributes are mapped to headers in the outgoing HTTP response.</p> <p>REQUEST_ATTRIBUTE The named AM attributes are mapped to request attributes in the outgoing HTTP response.</p> <p>HTTP_COOKIE The named AM attributes are mapped to cookies in the outgoing HTTP response.</p>
Default	NONE
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	AgentConfig.properties
AM console	<p>Tab: Application</p> <p>Title: Profile Attribute Fetch Mode</p>

Enable Attribute Encoding

When `true`, attribute values are URL-encoded before being set as a cookie.

Property name	<code>org.forgerock.agents.attribute.cookie.encode.enabled</code>
Aliases	<p><code>com.sun.identity.agents.config.attribute.cookie.encode</code> Introduced in Java Agent 5.0 <u>Recognized</u> from AM 6</p> <p><code>org.forgerock.agents.attribute.cookie.encode.enabled</code> Introduced in Java Agent 5.6</p>

Type	Boolean: true returns true; all other strings return false .
Default	true
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	AgentConfig.properties
AM console	Tab: Application Title: Enable Attribute Encoding Legacy title: Attribute Cookie Encode

Audit

Enable Local Audit Log Rotation

When `true` , rotate local audit log files that have reached the size specified by [Local Audit Log Rotation Size](#).

Property name	<code>org.forgerock.agents.local.audit.log.rotation.enabled</code>
Aliases	<code>org.forgerock.agents.local.audit.log.rotation.enabled</code> Introduced in Java Agent 5.6 <code>com.sun.identity.agents.config.local.log.rotate</code> Introduced in Java Agent 5.0 Recognized from AM 6
Type	Boolean: true returns true; all other strings return false .
Default	false
Bootstrap property	No
Required property	No

Restart required	No
Local configuration file	AgentConfig.properties
AM console	Tab: Global Title: Enable Local Audit Log Rotation Legacy title: Rotate Local Audit Log

Local Audit Log Rotation Size

The maximum size in bytes of the local audit log files. When [Enable Local Audit Log Rotation](#) is `true`, the agent rotates the log file when it reaches this size.

Property name	<code>org.forgerock.agents.local.audit.log.rotation.bytes</code>
Aliases	<code>com.sun.identity.agents.config.local.log.size</code> Introduced in Java Agent 5.0 Recognized from AM 6 <code>org.forgerock.agents.local.audit.log.rotation.bytes</code> Introduced in Java Agent 5.7
Type	Integer
Default	52428800
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	AgentConfig.properties
AM console	Tab: Global Title: Local Audit Log Rotation Size

Audit Logfile Retention Count

The number of audit log files to retain after rotation. When the specified limit is reached, the oldest file is deleted when a file rotation occurs.

When the value is `-1`, all rotated files are kept. When the value is, for example, `10`, the current file and nine older rotated files are kept.

Property name	<code>org.forgerock.agents.local.audit.log.retention.count</code>
Aliases	<code>org.forgerock.agents.local.audit.log.retention.count</code> Introduced in Java Agent 5.7 <u>Recognized</u> from AM 7
Type	Integer
Default	<code>-1</code>
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>
AM console	Tab: Global (from AM 7) Title: Audit Logfile Retention Count

Audit Access Types

The type of messages to audit.

Property name	<code>org.forgerock.agents.audit.what</code>
Aliases	<code>com.sun.identity.agents.config.audit.accesstype</code> Introduced in Java Agent 5.0 <u>Recognized</u> from AM 6 <code>org.forgerock.agents.audit.what</code> Introduced in Java Agent 5.6

Supported settings	<p>LOG_NONE Don't audit anything.</p> <p>LOG_ALLOW Audit only allowed requests.</p> <p>LOG_DENY Audit only denied requests.</p> <p>LOG_BOTH Audit both allowed and denied requests.</p>
Default	LOG_NONE
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	AgentConfig.properties
AM console	<p>Tab: Global</p> <p>Title: Audit Access Types</p>

Local Audit Log Filename

The full path to the agent's local audit log file.

Default: None; local auditing is disabled

Property name	org.forgerock.agents.local.audit.file.path
Aliases	<p>com.sun.identity.agents.config.local.logfile Introduced in Java Agent 5.0 <u>Recognized</u> from AM 7</p> <p>org.forgerock.agents.local.audit.file.path Introduced in Java Agent 5.6</p>
Type	String
Bootstrap property	Yes
Required property	No

Restart required	No
Local configuration file	AgentBootstrap.properties

Audit Log Location

The location where the agent logs audit messages. If [Audit Access Types](#) is LOG_NONE , this property has no effect.

Property name	org.forgerock.agents.audit.where
Aliases	com.sun.identity.agents.config.log.disposition Introduced in Java Agent 5.0 <u>Recognized</u> from AM 6 org.forgerock.agents.audit.where Introduced in Java Agent 5.6
Supported settings	NONE Don't audit anything, anywhere. LOCAL Audit locally only. REMOTE Audit remotely only. ALL Audit both locally and remotely.
Default	NONE
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	AgentConfig.properties
AM console	Tab: Global Title: Audit Log Location

Authentication failure

Authentication Fail Reason Parameter Name

A query parameter name to contain the reason why authentication failed. The agent appends this parameter to the URL or URI defined by [Authentication Fail URL](#).

If this property is not set, the agent does not append the reason for the authentication failure, when redirecting to the URL or URI.

To reduce the risk of leaking useful information, configure [Authentication Fail Reason Parameter Value Map](#) to change the strings for the above values.

Property name	<code>org.forgerock.agents.authn.fail.reason.parameter.name</code>
Aliases	<code>org.forgerock.agents.authn.fail.reason.parameter.name</code> Introduced in Java Agent 5.7 Recognized from AM 7
Type	String
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>
AM console	Tab: Miscellaneous (from AM 7) Title: Authentication Fail Reason Parameter Name

Authentication Fail Reason Parameter Value Map

After an authentication failure, malicious users can use the information you expose to gain access to the system. Map the reason for authentication failure to something generic, or something that is meaningful inside your organization.

When [Authentication Fail URL](#) is set, this property maps reasons for authentication failure to custom messages, as follows:

- `AUTHN_BOOKKEEPING_COOKIE_MISSING`: The agent cannot find the authentication tracking cookie. This error can happen if the user successfully authenticates, but clicks the back button of the browser to return to the previous page.

- **NONCE_MISSING** : The agent found the authentication tracking cookie, but it cannot find the unique identifier of the authentication request inside the cookie. This error can happen if the user successfully authenticates, but clicks the back button of the browser to return to the previous page.
- **BAD_AUDIENCE** : The audience in the JWT did not correspond to the audience in the cookie entry. This error can happen if all agents working in a cluster do not have the same Agent Profile Name.
- **NO_TOKEN** : The agent cannot find the session ID token.
- **TOKEN_EXPIRED** : The agent found the session ID token, but it is past its expiry date.
- **AM_SAYS_INVALID** : The agent found the session ID token, the expiry time is correct, but AM returns that the ID token is invalid.
- **JWT_INVALID** : The agent found the session ID token, but cannot parse it.
- **EXCEPTION** : The agent found the session ID token, but threw an exception while parsing it. Alternatively, the agent cannot connect to AM to validate the ID token, maybe due to a network outage.

Specify the authentication failure reason from the preceding table as the map key, and your custom error identifier string as the value. For example:

```
org.forgerock.agents.authn.fail.reason.remapper[TOKEN_EXPIRED]=MY_ERROR_MESSAGE
```

Consider remapping all the failure reasons to a new error message, then be specific on those that hold more meaning for your environment. For example:

```
org.forgerock.agents.authn.fail.reason.remapper=ERROR
```

```
org.forgerock.agents.authn.fail.reason.remapper[AUTHN_BOOKKEEPING_COOKIE_MISSING]=BACK_BUTTON_PRESSED
```

```
org.forgerock.agents.authn.fail.reason.remapper[NONCE_MISSING]=BACK_BUTTON_PRESSED
```

To map all the authentication failure reasons to the same message, you do not need to specify a key in the property.

Property name	org.forgerock.agents.authn.fail.reason.remapper
Aliases	org.forgerock.agents.authn.fail.reason.remapper Introduced in Java Agent 5.7 <u>Recognized</u> from AM 7

Type	Map <ul style="list-style-type: none"> • Keys: failed auth reason code • Values: masked value
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	AgentConfig.properties
AM console	Tab: Miscellaneous (from AM 7) Title: Authentication Fail Reason Parameter Value Map

Authentication Fail URL

The URL or URI to which the agent redirects the user after a failed authentication.

If this property is not set, the agent redirects the user to the URL defined in [Goto URL](#). If neither property is set, the agent returns an HTTP 400 Bad Request.

To configure the agent to send the reason for authentication failure in a named query parameter, configure [Authentication Fail Reason Parameter Name](#).

Property name	org.forgerock.agents.authn.fail.url
Aliases	org.forgerock.agents.authn.fail.url Introduced in Java Agent 5.7 Recognized from AM 7
Type	String
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	AgentConfig.properties

AM console	Tab: Miscellaneous (from AM 7) Title: Authentication Fail URL Legacy title: Authentication Fail Reason Url
------------	--

Goto URL

When [Authentication Fail URL](#) is not set, this property sets the URL or URI to which the agent redirects the user after a failed authentication. If neither property is set, the agent returns an HTTP 400 Bad Request.

To configure the agent to send the reason for authentication failure in a named query parameter, configure [Authentication Fail Reason Parameter Name](#).

Property name	<code>org.forgerock.agents.default.goto.url</code>
Aliases	<code>com.sun.identity.agents.config.openam.agent.default_goto_url</code> Introduced in Java Agent 5.0 <u>Recognized</u> from AM 7 <code>org.forgerock.agents.default.goto.url</code> Introduced in Java Agent 5.7
Type	String
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>
AM console	Tab: Miscellaneous (from AM 7) Title: Goto URL

Authentication service

AM Authentication Service Path

The path to the AM server.

Property name	<code>org.forgerock.agents.am.path</code>
Aliases	<code>com.ipplanet.am.services.deploymentDescriptor</code> Introduced in Java Agent 5.0 <code>org.forgerock.agents.am.path</code> Introduced in Java Agent 5.6
Type	String
Bootstrap property	Yes
Required property	Yes - If this property is missing, the agent fails to start
Restart required	Yes - Restart the container after changing the property
Local configuration file	<code>AgentBootstrap.properties</code>

AM Authentication Service Protocol

The protocol used by the AM server. Set to one of the following values:

- HTTP
- HTTPS

Property name	<code>org.forgerock.agents.am.protocol</code>
Aliases	<code>org.forgerock.agents.am.protocol</code> Introduced in Java Agent 5.6 <code>com.ipplanet.am.server.protocol</code> Introduced in Java Agent 5.0 <u>Recognized</u> from AM 6
Type	String
Bootstrap property	Yes
Required property	Yes - If this property is missing, the agent fails to start
Restart required	Yes - Restart the container after changing the property
Local configuration file	<code>AgentBootstrap.properties</code>

AM console	Tab: AM Services Title: AM Authentication Service Protocol
------------	---

Encryption Key/Salt

The key/salt used by the default encryption class to perform encryption and decryption within the agent.

Generate a secure, random key with `agentadmin --key` or `agentadmin --rotate` commands as described in [Rotate the agent profile password](#).

If this property is not set, the agent terminates with a configuration error.

WARNING

If changing this property manually, or with `agentadmin --key`, you must re-encrypt the agent profile password by using `agentadmin --encrypt`.

Property name	<code>org.forgerock.agents.encryption.key</code>
Aliases	<code>org.forgerock.agents.encryption.key</code> Introduced in Java Agent 5.10.1 <u>Recognized</u> from AM 7.1 <code>am.encryption.pwd</code> Introduced in Java Agent 5.0 <code>com.sun.identity.client.encryptionKey</code> Introduced in Java Agent 5.0
Type	String
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>

AM Authentication Service Host Name

The AM server host name.

Property name	<code>org.forgerock.agents.am.hostname</code>
Aliases	<code>com.ip1anet.am.server.host</code> Introduced in Java Agent 5.0 <u>Recognized</u> from AM 6 <code>org.forgerock.agents.am.hostname</code> Introduced in Java Agent 5.6
Type	String
Bootstrap property	Yes
Required property	Yes - If this property is missing, the agent fails to start
Restart required	Yes - Restart the container after changing the property
Local configuration file	<code>AgentBootstrap.properties</code>
AM console	Tab: AM Services Title: AM Authentication Service Host Name

AM Authentication Service Port

The AM server port number.

Property name	<code>org.forgerock.agents.am.port</code>
Aliases	<code>com.ip1anet.am.server.port</code> Introduced in Java Agent 5.0 <u>Recognized</u> from AM 6 <code>org.forgerock.agents.am.port</code> Introduced in Java Agent 5.6
Type	String
Bootstrap property	Yes
Required property	Yes - If this property is missing, the agent fails to start
Restart required	Yes - Restart the container after changing the property
Local configuration file	<code>AgentBootstrap.properties</code>

AM console	Tab: AM Services Title: AM Authentication Service Port
------------	---

Client identification

Client Hostname Header

The name of the HTTP header used to determine the hostname of a client. See also [Client IP Address Header](#).

If this property is not set, the value returned by `HttpServletRequest.getRemoteHost` is used.

Property name	<code>org.forgerock.agents.http.header.containing.remote.hostname</code>
Aliases	<code>org.forgerock.agents.http.header.containing.remote.hostname</code> Introduced in Java Agent 5.6 <code>com.sun.identity.agents.config.client.hostname.header</code> Introduced in Java Agent 5.0 Recognized from AM 6
Type	String
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>
AM console	Tab: Advanced Title: Client Hostname Header

Client IP Validation Mode

For each authenticated request from a named web application, check that the IP address of the request satisfies one of the following acceptance criteria:

- It originates from the IP address used for first authentication.
- It has acceptable changes only, as mapped in [Client IP Validation Address Map](#)
- If the web application is not named, check the the IP address globally, for all web applications.

Property name	<code>org.forgerock.agents.original.ip.check.mode.map</code>
Aliases	<code>org.forgerock.agents.original.ip.check.mode.map</code> Introduced in Java Agent 5.8.0 Recognized from AM 7.1
Supported settings	OFF IP address checking is disabled. DENY An "unacceptable" IP address change triggers an HTTP 403 response. LOGOUT An "unacceptable" IP address change causes the agent to invalidate the user token by calling the logout endpoint in AM and killing the user's cookies.
Default	OFF
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>
AM console	Tab: Application (from AM 7.1) Title: Client IP Validation Mode

Client IP Validation Address Map

A map of acceptable alternative values for IP addresses, or address ranges in CIDR format, that incoming requests may change to without triggering DENY or LOGOUT behaviour.

This property is used by [Client IP Validation Mode](#).

Property name	<code>org.forgerock.agents.acceptable.ip.address.map</code>
Aliases	<code>org.forgerock.agents.acceptable.ip.address.map</code> Introduced in Java Agent 5.8.0 Recognized from AM 7.1
Type	Map <ul style="list-style-type: none">• Keys: web application• Values: acceptable IP addresses, comma separated, CIDR format acceptable
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>
AM console	Tab: Application (from AM 7.1) Title: Client IP Validation Address Map

Client IP Address Header

The name of the HTTP header used to determine the IP address of a client. See also [Client Hostname Header](#).

If this property is not set, the value returned by `HttpServletRequest.getRemoteAddr` is used.

Property name	<code>org.forgerock.agents.http.header.containing.ip.address</code>
Aliases	<code>com.sun.identity.agents.config.client.ip.header</code> Introduced in Java Agent 5.0 Recognized from AM 6 <code>org.forgerock.agents.http.header.containing.ip.address</code> Introduced in Java Agent 5.6

Type	String
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	AgentConfig.properties
AM console	Tab: Advanced Title: Client IP Address Header

Connection pooling

Max HTTP Connection Count

When [Enable Connection Pooling](#) is `true`, this property defines the maximum number of HTTP connections allowed at any time.

Property name	<code>org.forgerock.agents.http.client.max.connections</code>
Aliases	<code>org.forgerock.agents.http.client.max.connections</code> Introduced in Java Agent 5.8.0
Type	Integer
Default	1000
Bootstrap property	Yes
Required property	No
Restart required	Yes - Restart the container after changing the property
Local configuration file	AgentBootstrap.properties
AM console	Tab: Redirect Title: Max HTTP Connection Count

HTTP Connection Timeout

When Enable Connection Pooling is `true`, this property defines the connection timeout in seconds.

Property name	<code>org.forgerock.agents.http.client.connection.timeout.seconds</code>
Aliases	<code>org.forgerock.agents.http.client.connection.timeout.seconds</code> Introduced in Java Agent 5.8.0
Type	Integer
Default	10
Bootstrap property	Yes
Required property	No
Restart required	Yes - Restart the container after changing the property
Local configuration file	<code>AgentBootstrap.properties</code>
AM console	Tab: Redirect Title: HTTP Connection Timeout

Enable HTTP Connection Reuse

When Enable Connection Pooling is `true`, this property enables connection reuse.

Property name	<code>org.forgerock.agents.http.client.reuse.connections.enabled</code>
Aliases	<code>org.forgerock.agents.http.client.reuse.connections.enabled</code> Introduced in Java Agent 5.8.0
Type	Boolean: <code>true</code> returns true; all other strings return false.
Default	<code>true</code>
Bootstrap property	Yes
Required property	No

Restart required	Yes - Restart the container after changing the property
Local configuration file	AgentBootstrap.properties

Enable HTTP Connection State

This option only applies when these properties are `true` :

- [Enable Connection Pooling](#)
- [Enable HTTP Connection Reuse](#)

Set this property to `true` to change the Apache HTTP Client default behavior, and allow connection reuse.

Because the client certificate is defined at the client level, all requests to the same target share the same client certificate, so enabling this property should not be an issue.

Property name	<code>org.forgerock.agents.http.client.connection.state.enabled</code>
Aliases	<code>org.forgerock.agents.http.client.connection.state.enabled</code> Introduced in Java Agent 5.8.0
Type	Boolean: <code>true</code> returns true; all other strings return <code>false</code> .
Default	<code>true</code>
Bootstrap property	Yes
Required property	No
Restart required	Yes - Restart the container after changing the property
Local configuration file	AgentBootstrap.properties

Enable Connection Pooling

When `true`, the agent uses connection pooling. Use connection pooling to improve performance when AM is available over low bandwidth connections, or to throttle the maximum number of connections made by the agent.

When AM is available over high bandwidth connections, connection pooling can reduce performance.

Property name	<code>org.forgerock.agents.use.connection.pooling.enabled</code>
Aliases	<code>org.forgerock.agents.use.connection.pooling.enabled</code> Introduced in Java Agent 5.8.0
Type	Boolean: <code>true</code> returns true; all other strings return <code>false</code> .
Default	<code>false</code>
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>

HTTP Socket Timeout

When Enable Connection Pooling is `true`, this property defines the socket timeout in seconds.

Property name	<code>org.forgerock.agents.http.client.socket.timeout.seconds</code>
Aliases	<code>org.forgerock.agents.http.client.socket.timeout.seconds</code> Introduced in Java Agent 5.8.0
Type	Integer
Default	<code>10</code>
Bootstrap property	Yes
Required property	No
Restart required	Yes - Restart the container after changing the property
Local configuration file	<code>AgentBootstrap.properties</code>

Enable HTTP Retry

When [Enable Connection Pooling](#) is `true`, this property enables retries after failed requests.

Property name	<code>org.forgerock.agents.http.client.retry.requests.enabled</code>
Aliases	<code>org.forgerock.agents.http.client.retry.requests.enabled</code> Introduced in Java Agent 5.8.0
Type	Boolean: <code>true</code> returns true; all other strings return <code>false</code> .
Default	<code>true</code>
Bootstrap property	Yes
Required property	No
Restart required	Yes - Restart the container after changing the property
Local configuration file	<code>AgentBootstrap.properties</code>

Container

Container Character Encoding

The character encoding used by the agent when encoding extended characters in the resource paths of not-enforced rules.

Property name	<code>org.forgerock.agents.container.encoding</code>
Aliases	<code>org.forgerock.agents.container.encoding</code> Introduced in Java Agent 5.9.1
Type	String
Default	UTF-8
Bootstrap property	No
Required property	No

Restart required	No
Local configuration file	AgentConfig.properties

Container Parameter Encoding

The character encoding used by the agent when encoding extended characters in the HTTP query parameters of not-enforced rules.

Property name	org.forgerock.agents.container.param.encoding
Aliases	org.forgerock.agents.container.param.encoding Introduced in Java Agent 5.9.1
Type	String
Default	ISO-8859-1
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	AgentConfig.properties

Continuous security

Continuous Security Cookie Map

Maps cookie values available in inbound resource requests to entries in the environmental conditions map, which agents send to AM during policy evaluation.

Property name	org.forgerock.agents.continuous.security.cookies .map
---------------	--

Aliases	<p><code>org.forgerock.agents.continuous.security.cookies.map</code> Introduced in Java Agent 5.6</p> <p><code>org.forgerock.openam.agents.config.continuous.security.cookies</code> Introduced in Java Agent 5.0 <u>Recognized</u> from AM 6</p>
Type	<p>Map</p> <ul style="list-style-type: none"> • Keys: incoming cookie name • Values: name of entry in environment map
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>
AM console	<p>Tab: Application</p> <p>Title: Continuous Security Cookie Map</p> <p>Legacy title: Continuous Security Cookies</p>

Continuous Security Header Map

Maps header values in inbound resource requests to entries in the environmental conditions map, which agents send to AM during policy evaluation.

Example:

```
org.forgerock.agents.continuous.security.headers.map[User-Agent]=myUserAgentHeaderEntry
```

Property name	<code>org.forgerock.agents.continuous.security.headers.map</code>
---------------	---

Aliases	<p><code>org.forgerock.agents.continuous.security.headers.map</code> Introduced in Java Agent 5.6</p> <p><code>org.forgerock.openam.agents.config.continuous.security.headers</code> Introduced in Java Agent 5.0 <u>Recognized</u> from AM 6</p>
Type	<p>Map</p> <ul style="list-style-type: none"> • Keys: incoming header name • Values: name of entry in environment map
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>
AM console	<p>Tab: Application</p> <p>Title: Continuous Security Header Map</p> <p>Legacy title: Continuous Security Headers</p>

Client Hostname Header

The name of the HTTP header used to determine the hostname of a client. See also [Client IP Address Header](#).

If this property is not set, the value returned by `HttpServletRequest.getRemoteHost` is used.

Property name	<code>org.forgerock.agents.http.header.containing.remote.hostname</code>
---------------	--

Aliases	<p><code>org.forgerock.agents.http.header.containing.remote.hostname</code> Introduced in Java Agent 5.6</p> <p><code>com.sun.identity.agents.config.client.hostname.header</code> Introduced in Java Agent 5.0 <u>Recognized</u> from AM 6</p>
Type	String
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>
AM console	<p>Tab: Advanced</p> <p>Title: Client Hostname Header</p>

Client IP Address Header

The name of the HTTP header used to determine the IP address of a client. See also [Client Hostname Header](#).

If this property is not set, the value returned by `HttpServletRequest.getRemoteAddr` is used.

Property name	<code>org.forgerock.agents.http.header.containing.ip.address</code>
Aliases	<p><code>com.sun.identity.agents.config.client.ip.header</code> Introduced in Java Agent 5.0 <u>Recognized</u> from AM 6</p> <p><code>org.forgerock.agents.http.header.containing.ip.address</code> Introduced in Java Agent 5.6</p>
Type	String
Bootstrap property	No

Required property	No
Restart required	No
Local configuration file	AgentConfig.properties
AM console	Tab: Advanced Title: Client IP Address Header

Cookie

Maximum Decompression Size

The maximum size, in bytes, a compressed cookie is allowed to expand to when decompressed.

Property name	org.forgerock.agents.max.decompression.size.bytes
Aliases	org.forgerock.agents.max.decompression.size.bytes Introduced in Java Agent 5.10.0
Type	Integer
Default	32768
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	AgentConfig.properties

Pre-Authn and Post Data Preservation Cookie Signing Value

The key to sign pre-authentication cookies and POST data preservation cookies.

The key is set during installation, when the agent requests the path to a file containing the cookie signing key, and then uses the key to set the cookie signing value in the

AgentKey.properties file. For information about how to set or change the key after installation, see [Rotate cookie signing keys](#).

For security, you are recommended to configure cookie signing. The agent does not sign cookies when:

- The path to the signing key is left blank during installation.
- The signing key in the AgentKey.properties file is less than 64-characters long.

Property name	org.forgerock.agents.cookie.signing.value
Aliases	org.forgerock.agents.cookie.signing.value Introduced in Java Agent 5.10.0
Type	String
Bootstrap property	No
Required property	No
Restart required	Yes - Restart the container after changing the property
Local configuration file	AgentKey.properties

Max Age of Pre-Authentication Cookie

The maximum age in seconds of the pre-authentication cookie configured in [Pre-Authentication Cookie Name](#).

Property name	org.forgerock.agents.authn.cookie.max.age.seconds
Aliases	org.forgerock.agents.authn.cookie.max.age.seconds Introduced in Java Agent 5.6.3.0 Recognized from AM 7
Type	Integer
Default	600
Bootstrap property	No
Required property	No
Restart required	No

Local configuration file	AgentConfig.properties
AM console	Tab: Global (from AM 7) Title: Max Age of Pre-Authentication Cookie Legacy title: Pre-Authenticated Cookie Max Age

Load Balancer Cookie Name

The load balancer cookie name. Make sure that this property has the same value as the AM property `com.ipplanet.am.lbcookie.name`.

Property name	<code>org.forgerock.agents.load.balancer.cookie.name</code>
Aliases	<code>org.forgerock.agents.load.balancer.cookie.name</code> Introduced in Java Agent 5.8.0 <u>Recognized</u> from AM 7.1
Type	String
Default	<code>amlbcookie</code>
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	AgentConfig.properties
AM console	Tab: Global (from AM 7.1) Title: Load Balancer Cookie Name

Enable Encoded Cookies

When `true`, cookies are base64-encoded.

Property name	<code>com.ipplanet.am.cookie.encode</code>
Aliases	<code>com.ipplanet.am.cookie.encode</code> Introduced in Java Agent 5.6 <u>Recognized</u> from AM 7

Type	Boolean: true returns true; all other strings return false .
Default	false
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	AgentConfig.properties
AM console	Tab: SSO (from AM 7) Title: Enable Encoded Cookies Legacy title: Encode Cookies

Enable HTTP Only Cookies

When true , cookies are flagged as HTTPOnly . Use this property to prevent scripts and third-party programs from accessing the cookies.

Property name	com.sun.identity.cookie.httponly
Aliases	com.sun.identity.cookie.httponly Introduced in Java Agent 5.0 <u>Recognized</u> from AM 7
Type	Boolean: true returns true; all other strings return false .
Default	true
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	AgentConfig.properties

AM console	Tab: SSO (from AM 7) Title: Enable HTTP Only Cookies Legacy title: Http Only
------------	--

Pre-Authentication Cookie Name

The name of the pre-authentication cookie. This cookie tracks the progress of authentication with AM, and protects requests from replay attacks. It contains the following information:

- URL of the original request
- HTTP mode
- Secure ID (subsequently baked into the nonce of the returned JWT)
- Relevant ACR information
- Transaction ID
- Expiry time configured by Max Age of Pre-Authentication Cookie

(Before Java Agent 5.7), The agent creates a single cookie containing records to identify all concurrent authentication requests to AM. In environments with lots of concurrent requests, or where the protected URLs are long, the cookie can reach the maximum size supported by the browser. When this happens, new authentication requests fail and the agent issues a 403 HTTP message to the user.

(Java Agent 5.7 and later versions) The agent can optionally create a cookie for each authentication request to AM. In some environments, this creates a large number of cookies. If you have tests in your environment that make multiple requests to AM from the same browser, you may find intermittent 403 HTTP messages; browsers can limit how many cookies they handle.

Configure the cookie name as follows:

- To use one cookie for all concurrent authentication requests to AM, configure as a string. For example, `org.forgerock.agents.authn.cookie.name=cookie-name`.
- To use one cookie for each authentication request to AM, configure as `%n`, or as `%n` before, in the middle of, or after a string. When the agent creates the cookie, it translates the string `%n` into a unique identifier. For example:
 - `org.forgerock.agents.authn.cookie.name=%n`
 - `org.forgerock.agents.authn.cookie.name=%n-cookie-name`
 - `org.forgerock.agents.authn.cookie.name=cookie-%n-name`

- `org.forgerock.agents.authn.cookie.name=cookie-name-%n`

The agent compresses and then signs the cookie.

Property name	<code>org.forgerock.agents.authn.cookie.name</code>
Aliases	<code>com.sun.identity.agents.config.cdsso.cookie.name</code> Introduced in Java Agent 5.0 <u>Recognized</u> from AM 7 <code>org.forgerock.agents.authn.cookie.name</code> Introduced in Java Agent 5.6
Type	String
Default	<code>amFilterCDSSORequest</code>
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>
AM console	Tab: Global (from AM 7) Title: Pre-Authentication Cookie Name Legacy title: Pre-Authenticated Cookie Name

Post Data Preservation Cookie Name

The name of the Post Data Preservation cookie. This cookie maintains the security of the data in unauthenticated POST requests. It contains a unique one-time code which is cross-checked against the stored data making it extremely difficult for malicious actors to replay the stored data for other users.

Since Java Agent 5.10, there is the option of creating one cookie for all concurrent PDP requests, or alternatively to have one uniquely named cookie per request.

If you have tests in your environment that make multiple PDP requests to the agent, you may find intermittent failures as browsers can limit how many cookies they handle.

Configure the cookie name as follows:

- To use one cookie for all concurrent PDP requests to AM, configure as a string. For example, `org.forgerock.agents.pdp.cookie.name=cookie-name`.
- To use one cookie for each authentication request to AM, configure as `%n` before, in the middle, or after a string. When the agent creates the cookie, it substitutes `%n` for a unique identifier. For example:
 - `org.forgerock.agents.pdp.cookie.name=%n`
 - `org.forgerock.agents.pdp.cookie.name=%n-cookie-name`
 - `org.forgerock.agents.pdp.cookie.name=cookie-%n-name`
 - `org.forgerock.agents.pdp.cookie.name=cookie-name-%n`

The agent compresses and then signs the cookie.

Property name	<code>org.forgerock.agents.pdp.cookie.name</code>
Aliases	<code>org.forgerock.agents.pdp.cookie.name</code> Introduced in Java Agent 5.10.0 <u>Recognized</u> from AM 7.1
Type	String
Default	PDP_Nonce
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	AgentConfig.properties

Enable Load Balancer Cookies

When `true`, the agent writes load balancer cookies each time it invokes AM.

Use this property with Load Balancer Cookie Name to improve performance. Load balancer cookies can reduce the number of calls that different AM instances make to the Core Token Service (CTS).

Because the agent invokes AM to log out a user, it creates a load-balancer cookie on logout. To remove these cookies on logout, add them to the Reset Cookie List.

Property name	<code>org.forgerock.agents.load.balancer.cookies.enabled</code>
---------------	---

Aliases	org.forgerock.agents.load balancer.cookies.enabled Introduced in Java Agent 5.8.0 <u>Recognized</u> from AM 7.1
Type	Boolean: true returns true; all other strings return false.
Default	false
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	AgentConfig.properties
AM console	Tab: Global (from AM 7.1) Title: Enable Load Balancer Cookies Legacy title: Load Balancer Cookie Enabled

Cookie reset

Reset Cookie List

A list of cookies to reset before redirecting the client for login, and when the client logs out. Cookie Reset must be true.

The agent searches for the cookie name using a case-sensitive search. If it finds a match, the cookie is reset. Otherwise, the agent searches again using a case-insensitive search. If it then finds a match, the cookie is reset and a warning is issued to the logs.

The list does not need to include the names of cookies created when Profile Attribute Fetch Mode or Session Attribute Fetch Mode has the value HTTP_COOKIE.

Property name	org.forgerock.agents.cookie.reset.name.list
---------------	---

Aliases	<p><code>org.forgerock.agents.cookie.reset.name.list</code> Introduced in Java Agent 5.6</p> <p><code>com.sun.identity.agents.config.cookie.reset.name</code> Introduced in Java Agent 5.0 <u>Recognized</u> from AM 6</p>
Type	List
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>
AM console	<p>Tab: SS0</p> <p>Title: Reset Cookie List</p> <p>Legacy title: Cookies Reset Name List</p>

Session Attribute Fetch Mode

Map the name of an AM session attribute specified in [Session Attribute Map](#) as follows:

- NONE: Do not map
- HTTP_HEADER: Map the to the name of an HTTP session header
- HTTP_COOKIE: Map to the name of an HTTP cookie
- REQUEST_ATTRIBUTE: Map to the name of an HTTP session attribute

When the value is `HTTP_COOKIE`, [Cookie Reset](#) is automatically set to `true`. Before redirecting the client for login, and when the client logs out, the agent resets profile and session attributes cookies, and cookies in the [Reset Cookie List](#).

Property name	<code>org.forgerock.agents.session.attribute.fetch.mode</code>
---------------	--

Aliases	<p><code>org.forgerock.agents.session.attribute.fetch.mode</code></p> <p>Introduced in Java Agent 5.6</p> <p><code>com.sun.identity.agents.config.session.attribute.fetch.mode</code></p> <p>Introduced in Java Agent 5.0</p> <p><u>Recognized</u> from AM 6</p>
Supported settings	<p>NONE</p> <p>No AM attributes are mapped.</p> <p>HTTP_HEADER</p> <p>The named AM attributes are mapped to headers in the outgoing HTTP response.</p> <p>REQUEST_ATTRIBUTE</p> <p>The named AM attributes are mapped to request attributes in the outgoing HTTP response.</p> <p>HTTP_COOKIE</p> <p>The named AM attributes are mapped to cookies in the outgoing HTTP response.</p>
Default	NONE
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>
AM console	<p>Tab: Application</p> <p>Title: Session Attribute Fetch Mode</p>

Cookie Reset

When `true`, the agent resets the cookies in the response before redirecting the client for login, and when the client logs out.

The agent resets the cookies listed in [Reset Cookie List](#), and cookies that store profile or session attributes (when [Profile Attribute Fetch Mode](#) or [Session Attribute Fetch Mode](#) has the value `HTTP_COOKIE`).

To reset cookies that store response attributes (when Response Attribute Fetch Mode has the value HTTP_COOKIE), add them to the Reset Cookie List.

Property name	org.forgerock.agents.cookie.reset.enabled
Aliases	org.forgerock.agents.cookie.reset.enabled Introduced in Java Agent 5.6 com.sun.identity.agents.config.cookie.reset.enable Introduced in Java Agent 5.0 <u>Recognized</u> from AM 6
Type	Boolean: true returns true; all other strings return false.
Default	false
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	AgentConfig.properties
AM console	Tab: SS0 Title: Cookie Reset

Reset Cookie Domain Map

Maps the cookie name specified in Reset Cookie List to a domain. After the cookie reset, the cookie is used in the domain.

Property name	org.forgerock.agents.cookie.reset.domain.map
Aliases	org.forgerock.agents.cookie.reset.domain.map Introduced in Java Agent 5.6 com.sun.identity.agents.config.cookie.reset.domain Introduced in Java Agent 5.0 <u>Recognized</u> from AM 6

Type	Map <ul style="list-style-type: none"> • Keys: cookie name • Values: cookie domain
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	AgentConfig.properties
AM console	Tab: SS0 Title: Reset Cookie Domain Map Legacy title: Cookies Reset Domain Map

Reset Cookie Path Map

Maps cookie name specified in [Reset Cookie List](#) to a path. After cookie reset, the cookie is used in the path.

Property name	org.forgerock.agents.cookie.reset.path.map
Aliases	com.sun.identity.agents.config.cookie.reset.path Introduced in Java Agent 5.0 <u>Recognized</u> from AM 6 org.forgerock.agents.cookie.reset.path.map Introduced in Java Agent 5.6
Type	Map <ul style="list-style-type: none"> • Keys: cookie name • Values: cookie path
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	AgentConfig.properties

AM console	Tab: SS0 Title: Reset Cookie Path Map Legacy title: Cookies Reset Path Map
------------	--

Profile Attribute Fetch Mode

Map the name of an AM profile attribute specified in [Profile Attribute Map](#) as follows:

- NONE: Do not map
- HTTP_HEADER: Map the to the name of an HTTP profile header
- HTTP_COOKIE: Map to the name of an HTTP cookie
- REQUEST_ATTRIBUTE: Map to the name of an HTTP profile attribute

Property name	<code>org.forgerock.agents.profile.attribute.fetch.mode</code>
Aliases	<code>com.sun.identity.agents.config.profile.attribute.fetch.mode</code> Introduced in Java Agent 5.0 <u>Recognized</u> from AM 6 <code>org.forgerock.agents.profile.attribute.fetch.mode</code> Introduced in Java Agent 5.6
Supported settings	<p>NONE No AM attributes are mapped.</p> <p>HTTP_HEADER The named AM attributes are mapped to headers in the outgoing HTTP response.</p> <p>REQUEST_ATTRIBUTE The named AM attributes are mapped to request attributes in the outgoing HTTP response.</p> <p>HTTP_COOKIE The named AM attributes are mapped to cookies in the outgoing HTTP response.</p>
Default	NONE

Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	AgentConfig.properties
AM console	Tab: Application Title: Profile Attribute Fetch Mode

Cross-domain single sign-on

Transmit Cookies Securely

When `true`, all cookies written by the agent are secure. For backward compatibility, the default is `false`.

Property name	<code>org.forgerock.agents.secure.cookies.enabled</code>
Aliases	<code>com.sun.identity.agents.config.cdsso.secure.enable</code> Introduced in Java Agent 5.0 <u>Recognized</u> from AM 6 <code>org.forgerock.agents.secure.cookies.enabled</code> Introduced in Java Agent 5.6 <code>com.ipplanet.am.cookie.secure</code> Introduced in Java Agent 5.0
Type	Boolean: <code>true</code> returns true; all other strings return <code>false</code> .
Default	<code>false</code>
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	AgentConfig.properties

AM console	Tab: SSO Title: Transmit Cookies Securely Legacy title: CDSSO Secure Enable
------------	---

Authentication Redirect URI

The URI the agent uses to process authentication requests.

When this property is not defined, the redirect URI is provided by AM.

When this property is defined and Location of Agent Configuration Repository is REMOTE , AM overwrites this property.

If OIDC authentication is being used, changing the value of this property while the agent is running prevents it from functioning. Restart the agent immediately after the value in AM is altered and the properties saved.

Property name	<code>org.forgerock.agents.authn.redirect.uri</code>
Aliases	<code>org.forgerock.agents.authn.redirect.uri</code> Introduced in Java Agent 5.6 <code>com.sun.identity.agents.config.cdsso.redirect.uri</code> Introduced in Java Agent 5.0 <u>Recognized</u> from AM 6
Type	String
Bootstrap property	No
Required property	No
Restart required	Yes - Restart the container after changing the property
Local configuration file	<code>AgentConfig.properties</code>
AM console	Tab: SSO Title: Authentication Redirect URI Legacy title: CDSSO Redirect URI

Cross-site scripting

XSS Code Element List

Strings that, when found in the request, cause the agent to redirect the client to an error page.

Property name	<code>org.forgerock.agents.xss.code.element.list</code>
Aliases	<code>org.forgerock.agents.xss.code.element.list</code> Introduced in Java Agent 5.7 <code>com.sun.identity.agents.config.xss.code.elements</code> Introduced in Java Agent 5.0 <u>Recognized</u> from AM 6
Type	List
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>
AM console	Tab: Advanced Title: XSS Code Element List Legacy title: Possible XSS code elements

XSS Redirect URI Map

A map of web application name to URI. When a cross-site scripting attack is detected, the agent redirects to the URI specified in the map. The URI is expected to be a page (HTML, or otherwise) indicating that such an attack has been detected.

For example, to redirect clients of MyApp to `/myapp/error.html`, enter MyApp as the map key and `/myapp/error.html` as the map value.

Property name	<code>org.forgerock.agents.xss.redirect.uri.map</code>
---------------	--

Aliases	<p><code>com.sun.identity.agents.config.xss.redirect.uri</code> Introduced in Java Agent 5.0 <u>Recognized</u> from AM 6</p> <p><code>org.forgerock.agents.xss.redirect.uri.map</code> Introduced in Java Agent 5.7</p>
Type	<p>Map</p> <ul style="list-style-type: none"> • Keys: web application • Values: cross site scripting URI
Default	<code>/agentapp/XSSCodeDetected.html</code>
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>
AM console	<p>Tab: Advanced</p> <p>Title: XSS Redirect URI Map</p> <p>Legacy title: XSS detection redirect URI</p>

Custom login redirect

Enable SSO Token Acceptance

Set this property as follows:

- `true` : Accept SSO tokens. Use this option when the agent and the token issuer are in the same domain, and for web applications and APIs where the backend accepts user information from SSO tokens.
- `false` : Do not accept SSO tokens; require OIDC JWTs for authentication.

During session upgrade the format of the composite advice is as follows:

- When both this property and Enable Custom Login Mode are `true` , the composite advice has the following format: ?
`authIndexType=composite_advice&authIndexValue=<Advices Value>`

- When either property is `false`, the composite advice has the following format: `? composite_advice=<Advices Value>`

Property name	<code>org.forgerock.agents.accept.sso.tokens.enabled</code>
Aliases	<code>org.forgerock.agents.accept.sso.tokens.enabled</code> Introduced in Java Agent 5.7.1 <u>Recognized</u> from AM 7.1 <code>org.forgerock.agents.accept.sso.tokens</code> Introduced in Java Agent 5.7.1 <code>com.forgerock.agents.accept.sso.tokens</code> Introduced in Java Agent 5.7.1
Type	Boolean: <code>true</code> returns true; all other strings return <code>false</code> .
Default	<code>false</code>
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>
AM console	Tab: SSO (from AM 7.1) Title: Enable SSO Token Acceptance Legacy title: Accept SSO Tokens

OAuth Login URL List

Use only when Enable Custom Login Mode is `false` and AM Login URL List is empty.

Specify rules to evaluate the incoming request URL, based on domain, path, request header, or query parameters. Specify a URL for login redirect with optional parameters.

Format, with no spaces between values:

```
[domain/path][header:value][?param=value[, param=value]]|[URL][?param=value&param=value]
```

When an unauthenticated request URL matches a rule specified by this property, the agent redirects the request to the specified URL for login.

When this property configures multiple rules, the agent sorts the rules into the following order and applies them in that order until it finds a match:

1. Header specification - a rule with a header specification is applied before other rules
2. Longest domain
3. Longest path
4. Highest number of parameter specifications

During redirect, the agent appends the goto parameter configured in Goto Parameter Name, and a nonce parameter, to the agent's CDSSO endpoint. If Enable FQDN Checking is `true`, the agent iterates through the list of URLs until it finds a redirect URL that matches the FQDN check values. Otherwise, the agent redirects the user to the URL configured in the conditional redirect rules.

[domain/path]

The incoming request URL:

- Domain: For example, `example.com`. The agent must match the domain and its subdomains. For example, `example.com` matches `mydomain.example.com` and `www.example.com`. Domains can also include path information, for example, `example.com/market`, but cannot specify ports.
- Subdomain: For example, `mydomain.example.com`. The agent match the domain, the subdomain, and any sub-subdomain. For example, `mydomain.example.com` matches `true.mydomain.example.com`. Subdomains can include path information, for example, `mydomain.example.com/secure`, but cannot specify ports.
- Path: For example, `/myapp`.
- No value: Nothing is specified before the `|` character and the rule applies to every incoming request.

[header:value]

One header/value pair provided in the incoming request. If the header value is not provided, the header can take any value. For example:

Requests containing a header called `X-local` with the value provided are redirected to the default URL:

```
org.forgerock.agents.oauth.login.url.list[0]= X-local:provided|
```

Requests containing a header called `X-local` with any value are redirected to the default URL:

```
org.forgerock.agents.oauth.login.url.list[0]= X-local:|
```

[?param=value[,param=value]

One or more parameter and value pairs provided in the incoming request. If the parameter value is not provided, the parameter can take any value. For example:

Requests containing a parameter called `site` with the value `shopping` are redirected to the default URL:

```
org.forgerock.agents.oauth.login.url.list[2]= ?site=shopping|
```

Requests containing a parameter called `target` with the value `cooking` **AND** a parameter called `price` with the value `low` are redirected to the default URL:+

```
org.forgerock.openam.agents.config.conditional.login.url[0]= ?  
target=cooking,price=low|
```

[URL]

The login URL. The URL can be an AM instance, an AM site, or a website other than AM.

Specify a URL in the format `protocol://FQDN[:port]/URI`, where the port is optional if it is 80 or 443. For example:

```
https://myweb.example.com/authApp/login.jsp
```

```
https://am.example.com:8443/openam/XUI/#login/
```

```
https://am.example.com:8443/openam/customlogin/login.jsp
```

If `[URL]` is not specified, the agent redirects the request to the AM instance or site specified by the following bootstrap properties:

```
org.forgerock.agents.am.protocol://org.forgerock.agents.am.hostname:org.forg  
erock.agents.am.port/org.forgerock.agents.am.path
```

[?param=value¶m=value]

One or more parameters to add to the login URL. Chain multiple parameters with an ampersand (&), for example, `realm=value¶meter1=value1¶meter2=value2`.

When the parameter is `?realm=value` it specifies the AM realm into which the agent logs the users. For example, `?realm=marketplace`.

When redirecting to AM's XUI, use an ampersand (&) instead of a question mark (?). For example,

```
https://am.example.com:8443/openam/XUI/#login/&realm=marketplace.
```

A realm parameter is not required in the login URL when any of the following conditions are true:

- The custom login page itself sets the realm parameter, for example, because it lets the user choose it. In this case, you must ensure the custom login page

always returns a realm parameter to the agent.

- The realm that the agent is logging the user into has DNS aliases configured in AM.
- AM logs the user into the realm whose DNS alias matches the incoming request URL. For example, an inbound request from the `http://marketplace.example.com` URL logs in the marketplace realm if the realm alias is set to `marketplace.example.com`.
- The users should always log in to the Top Level Realm.

Examples

+

Requests containing a header called `X-local` with the value `provided` are redirected to the specified URL in the `beta` realm:

+

```
org.forgerock.agents.oauth.login.url.list[0]= X-  
local:provided|http://mysite.local.com:8081/login?realm=beta
```

+

Requests containing a header called `X-local` with any value are redirected to the default URL in the `gamma` realm:

+

```
org.forgerock.agents.oauth.login.url.list[1]= X-local:|?realm=gamma
```

+

Requests containing a parameter called `site` with the value `shopping` **AND** a parameter called `mode` with the value `discount` are redirected to the default URL in the `discountshopping` realm:

+

```
org.forgerock.agents.oauth.login.url.list[2]= ?site=shopping,mode=discount|?  
realm=discountshopping
```

+

Requests containing a parameter called `target` with the value `cooking` are redirected to the AM XUI page in the `kitchen` realm. Note the use of `&` before the realm parameter:

+


```
org.forgerock.openam.agents.config.conditional.login.url[0]= ?
target=cooking|https://am.example.com:8443/openam/XUI/#login/&realm=kitchen
```

+

Requests containing a parameter called `target` with the value `cooking` are redirected to a non-AM login page in the `kitchen` realm. Note the use of `?` before the realm parameter:

+

```
org.forgerock.openam.agents.config.conditional.login.url[0]= ?
target=cooking|https://mysite.example.com:8443/login/?realm=kitchen
```

Property name	<code>org.forgerock.agents.oauth.login.url.list</code>
Aliases	<code>org.forgerock.agents.oauth.login.url.list</code> Introduced in Java Agent 5.6 <code>org.forgerock.openam.agents.config.conditional.login.url</code> Introduced in Java Agent 5.6 <u>Recognized</u> from AM 6
Type	List
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>
AM console	Tab: AM Services Title: OAuth Login URL List Legacy title: AM Conditional Login URL

Enable Custom Login Mode

Set the login redirection mode, as follows:

- `false`: Use default login redirection mode.
 - The agent can redirect requests to any AM instance that supports the `/oauth2/authorize` endpoint. By default, this is the AM instance that is

specified during installation.

- The `/oauth2/authorize` endpoint returns an OIDC ID token. This is the only response the agent accepts.
- Use with [OAuth Login URL List](#) to modify or redirect calls to the endpoint that provides the tokens.
- `true`: Use custom login redirection mode.
 - The agent handles JWTs or SSO tokens as session tokens for authentication and authorization, and can redirect login anywhere.
 - Use with [AM Login URL List](#) and [Legacy Login URL List](#) to modify or redirect calls.

During session upgrade, the format of the composite advice is as follows:

- When both this property and [Enable SSO Token Acceptance](#) are `true`, the composite advice has the following format: ?
`authIndexType=composite_advice&authIndexValue=<Advices Value>`
- When either property is `false`, the composite advice has the following format: ?
`composite_advice=<Advices Value>`

Property name	<code>org.forgerock.agents.legacy.login.enabled</code>
Aliases	<code>org.forgerock.agents.legacy.login.enabled</code> Introduced in Java Agent 5.6 <code>org.forgerock.openam.agents.config.allow.custom.login</code> Introduced in Java Agent 5.6 Recognized from AM 7
Type	Boolean: <code>true</code> returns true; all other strings return <code>false</code> .
Default	<code>false</code>
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>

AM console	Tab: AM Services (from AM 7) Title: Enable Custom Login Mode Legacy title: Allow Custom Login Mode
------------	--

AM Login URL List

The URL of the login page to use for authentication.

During the redirect, the agent appends the following parameters to the agent's CDSSO endpoint:

- The goto parameter configured in [Goto Parameter Name](#)
- A nonce parameter

Use the format `URL[?realm=realm_name?parameter1=value1&...]`, where:

- URL : URL of the login page to use for authentication
- `[?realm=realm_name¶meter1=value1&...]` : Optional parameters that the agent passes to the login page, for example, the AM realm at which to authenticate.

You do not need to specify an authentication realm if any of the following conditions are true:

- The custom login page sets the realm parameter, for example, because it lets the user choose the realm.
- The user authenticates into a realm that has DNS aliases configured in AM. AM then logs the user into the realm whose DNS alias matches the incoming request URL. For example, an inbound request from `http://marketplace.example.com` logs in the marketplace realm if the realm alias is set to `marketplace.example.com`.
- The user authenticates to the top-level realm.

This parameter can be overwritten by the custom login page if, for example, the user chooses the authentication realm.

Specify as many parameters your custom login pages require.

Example:

```
https://login.example.com/login.jsp?realm=marketplace&param1=value1
```

In some versions of AM you can configure more than one value for this property, but only the first value is honored.

Property name	com.sun.identity.agents.config.login.url
Aliases	com.sun.identity.agents.config.login.url Introduced in Java Agent 5.0 <u>Recognized</u> from AM 6
Type	List
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	AgentConfig.properties
AM console	Tab: AM Services Title: AM Login URL List Legacy title: AM Login URL

Login Reason Parameter Name

When Enable Custom Login Mode is `true`, this property specifies the name of a parameter included in calls to the custom login URL, to indicate why authentication is required. The parameter value can be used in a custom login page to provide additional feedback to the authenticating user.

If this property is specified, the agent includes a parameter named with the property value, and including one of the following values:

- `NO_TOKEN`: No token present in the original request.
- `TOKEN_EXPIRED`: Expiry time of the JWT was in the past.
- `EXCEPTION`: An unknown exception occurred, either while parsing the JWT or at some other stage of authentication.

To reduce the risk of leaking useful information, use the property Login Reason Value Map to change the strings for the above values.

For example, specifying

`org.forgerock.agents.login.reason.parameter.name=auth_reason` can cause the agent to redirect authentication to the following URL:

`https://custom.example.com:8443/.../login_endpoint?...
&auth_reason=TOKEN_EXPIRED&...`

Do not enter a value that clashes with other parameters used for authentication; for example, `realm` or `goto`.

Property name	<code>org.forgerock.agents.login.reason.parameter.name</code>
Aliases	<code>org.forgerock.agents.login.reason.parameter.name</code> Introduced in Java Agent 5.7
Type	String
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>
AM console	Tab: Miscellaneous (from AM 7) Title: Login Reason Parameter Name

Legacy Login URL List

Adds parameters conditionally to legacy login URLs.

Format, with no spaces between values:

`domain/path|url?param1=value1¶m2=value2`

Domain/path

The incoming request URL:

- **Domain:** For example, `example.com`. The agent must match the domain and its subdomains. For example, `example.com` matches `mydomain.example.com` and `www.example.com`. Domains can also include path information, for example, `example.com/market`, but cannot specify ports.
- **Subdomain:** For example, `mydomain.example.com`. The agent match the domain, the subdomain, and any sub-subdomain. For example, `mydomain.example.com` matches `true.mydomain.example.com`. Subdomains can include path information, for example, `mydomain.example.com/s6ecure`, but cannot specify ports.
- **Path:** For example, `/myapp`.
- **No value:** Nothing is specified before the `|` character and the rule applies to every incoming request.

URL

The URL to which redirect incoming login requests. The URL may be an AM instance, an AM site, or a website other than AM.

Specify a URL in the format `protocol://FQDN[:port]/URI`, where the port is optional if it is 80 or 443. For example:

```
https://myweb.example.com/authApp/login.jsp
```

```
https://am.example.com:8443/openam/XUI/#login/
```

```
https://am.example.com:8443/openam/customlogin/login.jsp
```

If the URL is not specified, the agent redirects the request to the AM instance or site specified by the following bootstrap properties:

```
org.forgerock.agents.am.protocol://org.forgerock.agents.am.hostname:org.f
orgerock.agents.am.port/org.forgerock.agents.am.path
```

¶meter1=value1

Parameters that can be added to the URL. Add as many parameters as your custom login pages need. Chain parameters with an & character, for example, `realm=value¶meter1=value1¶meter2=value2`.

Examples

```
org.forgerock.agents.legacy.login.url.list[0]=example.com|https://am.example
.com/openam/XUI/#login&realm=customers
```

```
org.forgerock.agents.legacy.login.url.list[1]=myapp.domain.com|https://login
.example.com/apps/login.jsp?realm=sales
```

```
org.forgerock.agents.legacy.login.url.list[2]=sales.example.com/marketplace|
?realm=marketplace
```

```
org.forgerock.agents.legacy.login.url.list[3]=|https://login.example.com/app
s/login.jsp?realm=sales&isblue=true&carowner=true
```

```
org.forgerock.agents.legacy.login.url.list[4]=|?realm=sales
```

Property name	<code>org.forgerock.agents.legacy.login.url.list</code>
Aliases	<code>org.forgerock.openam.agents.config.conditional.c ustom.login.url</code> Introduced in Java Agent 5.6 <u>Recognized</u> from AM 7 <code>org.forgerock.agents.legacy.login.url.list</code> Introduced in Java Agent 5.6

Type	List
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	AgentConfig.properties
AM console	Tab: AM Services (from AM 7) Title: Legacy Login URL List Legacy title: Custom Conditional Login URL

Default Login Redirect

OAuth Login URL List

Use only when Enable Custom Login Mode is `false` and AM Login URL List is empty.

Specify rules to evaluate the incoming request URL, based on domain, path, request header, or query parameters. Specify a URL for login redirect with optional parameters.

Format, with no spaces between values:

```
[domain/path][header:value][?param=value[, param=value]]|[URL][?param=value&param=value]
```

When an unauthenticated request URL matches a rule specified by this property, the agent redirects the request to the specified URL for login.

When this property configures multiple rules, the agent sorts the rules into the following order and applies them in that order until it finds a match:

1. Header specification - a rule with a header specification is applied before other rules
2. Longest domain
3. Longest path
4. Highest number of parameter specifications

During redirect, the agent appends the goto parameter configured in Goto Parameter Name, and a nonce parameter, to the agent's CDSSO endpoint. If Enable FQDN Checking is `true`, the agent iterates through the list of URLs until it finds a redirect URL that

matches the FQDN check values. Otherwise, the agent redirects the user to the URL configured in the conditional redirect rules.

[domain/path]

The incoming request URL:

- Domain: For example, `example.com`. The agent must match the domain and its subdomains. For example, `example.com` matches `mydomain.example.com` and `www.example.com`. Domains can also include path information, for example, `example.com/market`, but cannot specify ports.
- Subdomain: For example, `mydomain.example.com`. The agent match the domain, the subdomain, and any sub-subdomain. For example, `mydomain.example.com` matches `true.mydomain.example.com`. Subdomains can include path information, for example, `mydomain.example.com/s6ecure`, but cannot specify ports.
- Path: For example, `/myapp`.
- No value: Nothing is specified before the `|` character and the rule applies to every incoming request.

[header:value]

One header/value pair provided in the incoming request. If the header value is not provided, the header can take any value. For example:

Requests containing a header called `X-local` with the value provided are redirected to the default URL:

```
org.forgerock.agents.oauth.login.url.list[0]= X-local:provided|
```

Requests containing a header called `X-local` with any value are redirected to the default URL:

```
org.forgerock.agents.oauth.login.url.list[0]= X-local:|
```

[?param=value[,param=value]

One or more parameter and value pairs provided in the incoming request. If the parameter value is not provided, the parameter can take any value. For example:

Requests containing a parameter called `site` with the value `shopping` are redirected to the default URL:

```
org.forgerock.agents.oauth.login.url.list[2]= ?site=shopping|
```

Requests containing a parameter called `target`` with the value ``cooking` **AND** a parameter called `price` with the value `low` are redirected to the default URL:+

```
org.forgerock.openam.agents.config.conditional.login.url[0]= ?  
target=cooking,price=low|
```


[URL]

The login URL. The URL can be an AM instance, an AM site, or a website other than AM.

Specify a URL in the format `protocol://FQDN[:port]/URI`, where the port is optional if it is 80 or 443. For example:

```
https://myweb.example.com/authApp/login.jsp
```

```
https://am.example.com:8443/openam/XUI/#login/
```

```
https://am.example.com:8443/openam/customlogin/login.jsp
```

If [URL] is not specified, the agent redirects the request to the AM instance or site specified by the following bootstrap properties:

```
org.forgerock.agents.am.protocol://org.forgerock.agents.am.hostname:org.forgerock.agents.am.port/org.forgerock.agents.am.path
```

[?param=value¶m=value]

One or more parameters to add to the login URL. Chain multiple parameters with an ampersand (&), for example, `realm=value¶meter1=value1¶meter2=value2`.

When the parameter is `?realm=value` it specifies the AM realm into which the agent logs the users. For example, `?realm=marketplace`.

When redirecting to AM's XUI, use an ampersand (&) instead of a question mark (?). For example,

```
https://am.example.com:8443/openam/XUI/#login/&realm=marketplace.
```

A realm parameter is not required in the login URL when any of the following conditions are true:

- The custom login page itself sets the realm parameter, for example, because it lets the user choose it. In this case, you must ensure the custom login page always returns a realm parameter to the agent.
- The realm that the agent is logging the user into has DNS aliases configured in AM.
- AM logs the user into the realm whose DNS alias matches the incoming request URL. For example, an inbound request from the `http://marketplace.example.com` URL logs in the marketplace realm if the realm alias is set to `marketplace.example.com`.
- The users should always log in to the Top Level Realm.

Examples

+

Requests containing a header called `X-local` with the value provided are redirected to the specified URL in the `beta` realm:

+

```
org.forgerock.agents.oauth.login.url.list[0]= X-  
local:provided|http://mysite.local.com:8081/login?realm=beta
```

+

Requests containing a header called `X-local` with any value are redirected to the default URL in the `gamma` realm:

+

```
org.forgerock.agents.oauth.login.url.list[1]= X-local:|?realm=gamma
```

+

Requests containing a parameter called `site` with the value `shopping` **AND** a parameter called `mode` with the value `discount` are redirected to the default URL in the `discountshopping` realm:

+

```
org.forgerock.agents.oauth.login.url.list[2]= ?site=shopping,mode=discount|?  
realm=discountshopping
```

+

Requests containing a parameter called `target` with the value `cooking` are redirected to the AM XUI page in the `kitchen` realm. Note the use of `&` before the realm parameter:

+

```
org.forgerock.openam.agents.config.conditional.login.url[0]= ?  
target=cooking|https://am.example.com:8443/openam/XUI/#login/&realm=kitchen
```

+

Requests containing a parameter called `target` with the value `cooking` are redirected to a non-AM login page in the `kitchen` realm. Note the use of `?` before the realm parameter:

+

```
org.forgerock.openam.agents.config.conditional.login.url[0]= ?  
target=cooking|https://mysite.example.com:8443/login/?realm=kitchen
```

Property name	<code>org.forgerock.agents.oauth.login.url.list</code>
---------------	--

Aliases	<p><code>org.forgerock.agents.oauth.login.url.list</code> Introduced in Java Agent 5.6</p> <p><code>org.forgerock.openam.agents.config.conditional.login.url</code> Introduced in Java Agent 5.6 <u>Recognized</u> from AM 6</p>
Type	List
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>
AM console	<p>Tab: AM Services</p> <p>Title: OAuth Login URL List</p> <p>Legacy title: AM Conditional Login URL</p>

Enable Custom Login Mode

Set the login redirection mode, as follows:

- `false` : Use default login redirection mode.
 - The agent can redirect requests to any AM instance that supports the `/oauth2/authorize` endpoint. By default, this is the AM instance that is specified during installation.
 - The `/oauth2/authorize` endpoint returns an OIDC ID token. This is the only response the agent accepts.
 - Use with OAuth Login URL List to modify or redirect calls to the endpoint that provides the tokens.
- `true` : Use custom login redirection mode.
 - The agent handles JWTs or SSO tokens as session tokens for authentication and authorization, and can can redirect login anywhere.
 - Use with AM Login URL List and Legacy Login URL List to modify or redirect calls.

During session upgrade, the format of the composite advice is as follows:

- When both this property and [Enable SSO Token Acceptance](#) are true , the composite advice has the following format: ?
authIndexType=composite_advice&authIndexValue=<Advices Value>
- When either property is false , the composite advice has the following format: ?
composite_advice=<Advices Value>

Property name	org.forgerock.agents.legacy.login.enabled
Aliases	org.forgerock.agents.legacy.login.enabled Introduced in Java Agent 5.6 org.forgerock.openam.agents.config.allow.custom.login Introduced in Java Agent 5.6 Recognized from AM 7
Type	Boolean: true returns true; all other strings return false .
Default	false
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	AgentConfig.properties
AM console	Tab: AM Services (from AM 7) Title: Enable Custom Login Mode Legacy title: Allow Custom Login Mode

AM Login URL List

The URL of the login page to use for authentication.

During the redirect, the agent appends the following parameters to the agent's CDSSO endpoint:

- The goto parameter configured in [Goto Parameter Name](#)
- A nonce parameter

Use the format `URL[?realm=realm_name?parameter1=value1&...]` , where:

- URL : URL of the login page to use for authentication
- [?realm=realm_name¶meter1=value1&...] : Optional parameters that the agent passes to the login page, for example, the AM realm at which to authenticate.

You do not need to specify an authentication realm if any of the following conditions are true:

- The custom login page sets the realm parameter, for example, because it lets the user choose the realm.
- The user authenticates into a realm that has DNS aliases configured in AM. AM then logs the user into the realm whose DNS alias matches the incoming request URL. For example, an inbound request from `http://marketplace.example.com` logs in the marketplace realm if the realm alias is set to `marketplace.example.com`.
- The user authenticates to the top-level realm.

This parameter can be overwritten by the custom login page if, for example, the user chooses the authentication realm.

Specify as many parameters your custom login pages require.

Example:

`https://login.example.com/login.jsp?realm=marketplace¶m1=value1`

In some versions of AM you can configure more than one value for this property, but only the first value is honored.

Property name	<code>com.sun.identity.agents.config.login.url</code>
Aliases	<code>com.sun.identity.agents.config.login.url</code> Introduced in Java Agent 5.0 <u>Recognized</u> from AM 6
Type	List
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>
AM console	Tab: AM Services Title: AM Login URL List Legacy title: AM Login URL

Legacy Login URL List

Adds parameters conditionally to legacy login URLs.

Format, with no spaces between values:

```
domain/path|url?param1=value1&param2=value2
```

Domain/path

The incoming request URL:

- Domain: For example, `example.com`. The agent must match the domain and its subdomains. For example, `example.com` matches `mydomain.example.com` and `www.example.com`. Domains can also include path information, for example, `example.com/market`, but cannot specify ports.
- Subdomain: For example, `mydomain.example.com`. The agent match the domain, the subdomain, and any sub-subdomain. For example, `mydomain.example.com` matches `true.mydomain.example.com`. Subdomains can include path information, for example, `mydomain.example.com/s6ecure`, but cannot specify ports.
- Path: For example, `/myapp`.
- No value: Nothing is specified before the `|` character and the rule applies to every incoming request.

URL

The URL to which redirect incoming login requests. The URL may be an AM instance, an AM site, or a website other than AM.

Specify a URL in the format `protocol://FQDN[:port]/URI`, where the port is optional if it is 80 or 443. For example:

```
https://myweb.example.com/authApp/login.jsp
```

```
https://am.example.com:8443/openam/XUI/#login/
```

```
https://am.example.com:8443/openam/customlogin/login.jsp
```

If the URL is not specified, the agent redirects the request to the AM instance or site specified by the following bootstrap properties:

```
org.forgerock.agents.am.protocol://org.forgerock.agents.am.hostname:org.f  
orgerock.agents.am.port/org.forgerock.agents.am.path
```

¶meter1=value1

Parameters that can be added to the URL. Add as many parameters as your custom login pages need. Chain parameters with an `&` character, for example, `realm=value¶meter1=value1¶meter2=value2`.

Examples

```
org.forgerock.agents.legacy.login.url.list[0]=example.com|https://am.example.com/openam/XUI/#login&realm=customers
```

```
org.forgerock.agents.legacy.login.url.list[1]=myapp.domain.com|https://login.example.com/apps/login.jsp?realm=sales
```

```
org.forgerock.agents.legacy.login.url.list[2]=sales.example.com/marketplace|?realm=marketplace
```

```
org.forgerock.agents.legacy.login.url.list[3]=|https://login.example.com/apps/login.jsp?realm=sales&isblue=true&carowner=true
```

```
org.forgerock.agents.legacy.login.url.list[4]=|?realm=sales
```

Property name	org.forgerock.agents.legacy.login.url.list
Aliases	org.forgerock.openam.agents.config.conditional.custom.login.url Introduced in Java Agent 5.6 <u>Recognized</u> from AM 7 org.forgerock.agents.legacy.login.url.list Introduced in Java Agent 5.6
Type	List
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	AgentConfig.properties
AM console	Tab: AM Services (from AM 7) Title: Legacy Login URL List Legacy title: Custom Conditional Login URL

Deprecated

Debug File Rotation Size (deprecated)

Previously used to say when to rotate the log files based on file size. This should now be specified in the agent-logback.xml file in the agent config directory.

Default: Empty

Property name	<code>org.forgerock.agents.debug.rotation.size.bytes</code>
Aliases	<code>org.forgerock.agents.debug.rotation.size.bytes</code> Introduced in Java Agent 5.7 <code>org.forgerock.openam.debug.rotation.maxsize</code> Introduced in Java Agent 5.0 <u>Recognized</u> from AM 7
Type	String
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>
AM console	Tab: Global (from AM 7) Title: Debug File Rotation Size (deprecated)

Log File Directory (deprecated)

Previously used to specify where the log files were written. This should now be specified in the agent-logback.xml file in the agent config directory.

Property name	<code>com.ipplanet.services.debug.directory</code>
Aliases	<code>com.ipplanet.services.debug.directory</code> Introduced in Java Agent 5.0 <u>Recognized</u> from AM 7
Type	String
Bootstrap property	No
Required property	No
Restart required	No

Local configuration file	AgentConfig.properties
--------------------------	------------------------

Debug File Rotation Suffix (deprecated)

Previously used as the suffix for the log file name during rotation. This should now be specified in the agent-logback.xml file in the agent config directory.

Default: Empty

Property name	org.forgerock.agents.debug.suffix
Aliases	org.forgerock.openam.debug.suffix Introduced in Java Agent 5.0 <u>Recognized</u> from AM 7 org.forgerock.agents.debug.suffix Introduced in Java Agent 5.7
Type	String
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	AgentConfig.properties
AM console	Tab: Global (from AM 7) Title: Debug File Rotation Suffix (deprecated)

Debug File Rotation Retention Count (deprecated)

Previously used to define the number of retained log files. This should now be specified in the agent-logback.xml file in the agent config directory.

Property name	org.forgerock.agents.debug.retention.count
Aliases	org.forgerock.agents.debug.retention.count Introduced in Java Agent 5.7 <u>Recognized</u> from AM 7

Type	String
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	AgentConfig.properties
AM console	Tab: Global (from AM 7) Title: Debug File Rotation Retention Count (deprecated)

Debug File Rotation Time (deprecated)

Previously used to say when to rotate the log files based on time. This should now be specified in the agent-logback.xml file in the agent config directory.

Default: Empty

Property name	org.forgerock.agents.debug.rotation.time.minutes
Aliases	org.forgerock.openam.debug.rotation Introduced in Java Agent 5.0 <u>Recognized</u> from AM 7 org.forgerock.agents.debug.rotation.time.minutes Introduced in Java Agent 5.7
Type	String
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	AgentConfig.properties
AM console	Tab: Global (from AM 7) Title: Debug File Rotation Time (deprecated)

Debug File Rotation Prefix (deprecated)

Previously used as the prefix for the log file name. This should now be specified in the agent-logback.xml file in the agent config directory.

Default: Empty

Property name	org.forgerock.agents.debug.prefix
Aliases	org.forgerock.openam.debug.prefix Introduced in Java Agent 5.0 <u>Recognized</u> from AM 7 org.forgerock.agents.debug.prefix Introduced in Java Agent 5.7
Type	String
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	AgentConfig.properties
AM console	Tab: Global (from AM 7) Title: Debug File Rotation Prefix (deprecated)

Encryption

Encryption Class

The name of the class to be used by the Java agent to implement encryption and decryption. The class must implement both com.iplanet.services.util.AMEncryption and com.iplanet.services.util.ConfigurableKey

For details see [Rotate the agent profile password](#)

WARNING

After changing this property, you must re-encrypt the agent profile password.

Property name	org.forgerock.agents.encryptor.classname
---------------	--

Aliases	org.forgerock.agents.encryptor.classname Introduced in Java Agent 5.0 com.ipplanet.security.encryptor Introduced in Java Agent 5.0
Type	String
Default	org.forgerock.openam.shared.security.crypto.AESWRapEncryption
Bootstrap property	Yes
Required property	Yes - If this property is missing, the agent fails to start
Restart required	No
Local configuration file	AgentBootstrap.properties

Encryption Key/Salt

The key/salt used by the default encryption class to perform encryption and decryption within the agent.

Generate a secure, random key with `agentadmin --key` or `agentadmin --rotate` commands as described in [Rotate the agent profile password](#).

If this property is not set, the agent terminates with a configuration error.

WARNING

If changing this property manually, or with `agentadmin --key`, you must re-encrypt the agent profile password by using `agentadmin --encrypt`.

Property name	org.forgerock.agents.encryption.key
Aliases	org.forgerock.agents.encryption.key Introduced in Java Agent 5.10.1 Recognized from AM 7.1 am.encryption.pwd Introduced in Java Agent 5.0 com.sun.identity.client.encryptionKey Introduced in Java Agent 5.0

Type	String
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	AgentConfig.properties

Fragment

Fragment Relay URI

A URI to act as a dummy endpoint within the agent for capturing URL fragments in unauthenticated requests:

- When empty, unauthenticated requests to a URL with a fragment are authenticated and then redirected to the URL without the fragment.
- When set, unauthenticated requests are authenticated and then redirected to the requested URL. An extra redirect is incurred for all unauthenticated requests, to capture and process the URL fragment.

Use a dummy URI within the agent web application, such as `/agentapp/pre-authn-fragment-capture`. Avoid dummy URIs used for other purposes.

Property name	<code>org.forgerock.agents.authn.fragment.relay.uri</code>
Aliases	<code>org.forgerock.agents.authn.fragment.relay.uri</code> Introduced in Java Agent 5.7 <u>Recognized</u> from AM 7
Type	String
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	AgentConfig.properties
AM console	Tab: Advanced (from AM 7) Title: Fragment Relay URI

Fully qualified domain name

Default FQDN

The default FQDN to use when the agent cannot find a match in the [FQDN Map](#). If this property is not defined, [Enable FQDN Checking](#) is set to `false`.

Use this property to map requests with virtual, invalid, or partial hostnames to URLs that contain a correct FQDN.

Property name	<code>org.forgerock.agents.fqdn.default</code>
Aliases	<code>org.forgerock.agents.fqdn.default</code> Introduced in Java Agent 5.6 <code>com.sun.identity.agents.config.fqdn.default</code> Introduced in Java Agent 5.0 Recognized from AM 6
Type	String
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>
AM console	Tab: Global Title: Default FQDN Legacy title: FQDN Default

FQDN Map

Key:Value maps of incoming hostname to outgoing domain. Use this property to map requests with virtual, invalid, or partial hostnames to a correct FQDN.

This property requires [Enable FQDN Checking](#) to be `true`, and [Default FQDN](#) to be set to suitable default FQDN.

The agent maintains the following maps, which can each contain multiple entries:

- Map 1, where the key is the incoming hostname without wildcards, and the value is the outgoing domain.
- Map 2, where the key is the incoming hostname with wildcards (* or ?), and the value is the outgoing domain.

Map keys are case insensitive. Incoming hostnames are converted to lowercase before the agent maps them, and the agent automatically converts uppercase keys and values to lowercase before mapping.

The agent maps FQDNs as follows:

1. Searches map 1 for the incoming hostname. If there is a match, the agent redirects the request to the mapped value.
2. Searches map 2 for a pattern that matches the incoming hostname, iterating through the entries in random order. If there is a match, the agent redirects the request to the mapped value.
3. Redirects the request to the hostname in Default FQDN.

Examples:

```
org.forgerock.agents.fqdn.map[agent]=agent.localtest.me
```

```
org.forgerock.agents.fqdn.map[agent.virtualtest.me]=virtual-
host.localtest.me
```

```
org.forgerock.agents.fqdn.map[agent-*.localtest.me]=agent.localtest.me
```

Property name	org.forgerock.agents.fqdn.map
Aliases	com.sun.identity.agents.config.fqdn.mapping Introduced in Java Agent 5.0 <u>Recognized</u> from AM 6 org.forgerock.agents.fqdn.map Introduced in Java Agent 5.6
Type	Map <ul style="list-style-type: none"> • Keys: canonical name of invalid server • Values: canonical name of valid server
Bootstrap property	No
Required property	No
Restart required	No

Local configuration file	AgentConfig.properties
AM console	Tab: Global Title: FQDN Map Legacy title: FQDN Virtual Host Map

Enable FQDN Checking

When `true`, the agent compares the hostname of each request to the mappings in [FQDN Map](#).

- If it finds a match, it transforms the request URL to the mapped URL.
- If it doesn't find a match, it transforms the request URL to the value in [Default FQDN](#).

If [Default FQDN](#) is not set, this property is automatically set to `false`.

Property name	<code>org.forgerock.agents.fqdn.check.enabled</code>
Aliases	<code>com.sun.identity.agents.config.fqdn.check.enable</code> Introduced in Java Agent 5.0 Recognized from AM 6 <code>org.forgerock.agents.fqdn.check.enabled</code> Introduced in Java Agent 5.6
Type	Boolean: <code>true</code> returns true; all other strings return <code>false</code> .
Default	<code>true</code>
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	AgentConfig.properties
AM console	Tab: Global Title: Enable FQDN Checking Legacy title: FQDN Check

Global

Enable Prometheus Monitoring

When `true`, the agent is monitored by Prometheus. When `false`, the agent is not monitored by Prometheus.

Property name	<code>org.forgerock.agents.prometheus.monitoring.enabled</code>
Aliases	<code>org.forgerock.agents.prometheus.monitoring.enabled</code> Introduced in Java Agent 5.6
Type	Boolean: <code>true</code> returns true; all other strings return false.
Default	<code>true</code>
Bootstrap property	Yes
Required property	No
Restart required	No
Local configuration file	<code>AgentBootstrap.properties</code>
AM console	Tab: Monitoring Title: Enable Prometheus Monitoring

HTTP 302 Redirect Data

When [Enable HTTP 302 Redirects](#), this property specifies the data to return instead of an HTTP 302 Redirect.

Property name	<code>org.forgerock.agents.302.redirect.http.data</code>
Aliases	<code>org.forgerock.agents.302.redirect.http.data</code> Introduced in Java Agent 5.8.0 Recognized from AM 7.1
Type	String

Default	<pre>{ "redirect": { "requestUri": "%REQUEST_URI%", "requestUrl": "%REQUEST_URL%", "targetUrl": "%TARGET%" } }</pre>
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	AgentConfig.properties
AM console	Tab: Miscellaneous (from AM 7.1) Title: HTTP 302 Redirect Data

HTTP 302 Redirect Not-Enforced List

When [Enable HTTP 302 Redirects](#), this property specifies a list of URLs for which HTTP 302 Redirect does not take place.

If a request matches an entry in the list, HTTP 302 Redirect does not take place for that request, and the agent returns a block of configurable JSON.

Property name	<code>org.forgerock.agents.config.json.url</code>
Aliases	<code>org.forgerock.agents.config.json.url</code> Introduced in Java Agent 5.8.0 <code>org.forgerock.agents.302.redirect.ner.list</code> Introduced in Java Agent 5.8.0 Recognized from AM 7.1
Type	List
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	AgentConfig.properties

AM console	Tab: Miscellaneous (from AM 7.1) Title: HTTP 302 Redirect Not-Enforced List Legacy title: HTTP 302 Redirect Not Enforced List
------------	---

HTTP 302 Redirect Replacement HTTP Status Code

When Enable HTTP 302 Redirects is false, this property specifies the HTTP code to return instead of an HTTP 302 (Redirect).

Property name	<code>org.forgerock.agents.302.redirect.http.status.code</code>
Aliases	<code>org.forgerock.agents.302.redirect.http.status.code</code> Introduced in Java Agent 5.8.0 <u>Recognized</u> from AM 7.1 <code>org.forgerock.agents.config.json.response.code</code> Introduced in Java Agent 5.8.0
Type	Integer
Default	200
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>
AM console	Tab: Miscellaneous (from AM 7.1) Title: HTTP 302 Redirect Replacement HTTP Status Code Legacy title: HTTP 302 Redirect Replacement HTTP Code

Goto Parameter Name

Renames the `goto` parameter. During redirection, the agent appends the requested URL to the named parameter.

Use this property when your web application requires a parameter other than `goto`.

In the following example, the parameter is renamed to `goto2`:

```
com.sun.identity.agents.config.redirect.param=goto2
```

The redirection URL becomes like this:

```
https://www.example.com:8443/accessDenied.html?  
goto2=http%3A%2F%www.example.com%3A8020%managers%2Findex.jsp
```

The URL appended to the `goto2` parameter is the URL that the user tried to access when the agent redirected the request to the `accessDenied.html` page, configured with [Access Denied URI Map](#).

Property name	<code>com.sun.identity.agents.config.redirect.param</code>
Aliases	<code>com.sun.identity.agents.config.redirect.param</code> Introduced in Java Agent 5.0 Recognized from AM 6
Type	String
Default	<code>goto</code>
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>
AM console	Tab: Miscellaneous Title: Goto Parameter Name

HTTP 302 Redirect Content Type

When [Enable HTTP 302 Redirects](#), this property specifies the content type of the data to return instead of an HTTP 302 Redirect.

Property name	<code>org.forgerock.agents.302.redirect.http.content.type</code>
---------------	--

Aliases	<code>org.forgerock.agents.302.redirect.http.content.type</code> Introduced in Java Agent 5.8.0 <u>Recognized</u> from AM 7.1
Type	String
Default	<code>application/json</code>
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>
AM console	Tab: Miscellaneous (from AM 7.1) Title: HTTP 302 Redirect Content Type

HTTP 302 Redirect Invert Not-Enforced List

When Enable HTTP 302 Redirects is `false`, and this property is `true`, the agent inverts the meaning of HTTP 302 Redirect Not-Enforced List, so that it specifies a list of URLs for which HTTP 302 Redirect does take place.

Property name	<code>org.forgerock.agents.config.json.url.invert</code>
Aliases	<code>org.forgerock.agents.config.json.url.invert</code> Introduced in Java Agent 5.8.0 <code>org.forgerock.agents.302.redirect.invert.enabled</code> Introduced in Java Agent 5.8.0 <u>Recognized</u> from AM 7.1
Type	Boolean: <code>true</code> returns true; all other strings return <code>false</code> .
Default	<code>false</code>
Bootstrap property	No
Required property	No
Restart required	No

Local configuration file	AgentConfig.properties
AM console	Tab: Miscellaneous (from AM 7.1) Title: HTTP 302 Redirect Invert Not-Enforced List

Enable HTTP 302 Redirects

Controls how the agent handles redirects, as follows:

- `true`: HTTP 302 Redirects are enabled. When an unauthenticated request is made, and not-enforced rules do not apply, the agent returns an HTTP 302 code to redirect the user to an authentication endpoint.
- `false`: HTTP 302 Redirects are disabled. When an unauthenticated request is made, the agent returns a block of configurable JSON that can be intercepted.

The returned HTTP code, content type, and data is configured by the following properties

- [HTTP 302 Redirect Replacement HTTP Status Code](#)
- [HTTP 302 Redirect Content Type](#)
- [HTTP 302 Redirect Data](#)

Lists of URLs in a `not-enforced` rule style, for which the data is produced are configured by the following properties

- [HTTP 302 Redirect Not-Enforced List](#)
- [HTTP 302 Redirect Invert Not-Enforced List](#)

Use this option when it is difficult to handle 302, for example, when the agent is accessed by a JavaScript application, or by something other than a browser.

Property name	<code>org.forgerock.agents.302.redirects.enabled</code>
Aliases	<code>org.forgerock.agents.302.redirects.enabled</code> Introduced in Java Agent 5.8.0 Recognized from AM 7.1
Type	Boolean: <code>true</code> returns true; all other strings return <code>false</code> .
Default	<code>true</code>
Bootstrap property	No

Required property	No
Restart required	No
Local configuration file	AgentConfig.properties
AM console	Tab: Miscellaneous (from AM 7.1) Title: Enable HTTP 302 Redirects Legacy title: HTTP 302 Redirects Enabled

Legacy support

Enable Legacy Support Handlers (deprecated)

A flag to enable or disable the inbound and outbound legacy support handlers within the agent.

Property name	org.forgerock.agents.legacy.support.enabled
Deprecated in	5.6
Aliases	com.sun.identity.agents.config.legacy.support.enable Introduced in Java Agent 5.0 <u>Recognized</u> from AM 6 org.forgerock.agents.legacy.support.enabled Introduced in Java Agent 5.6
Type	Boolean: true returns true; all other strings return false.
Default	false
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	AgentConfig.properties

AM console	Tab: Miscellaneous Title: Enable Legacy Support Handlers Legacy title: Legacy User Agent Support Enable
------------	---

Legacy User Agent Redirect URI (deprecated)

A URI that triggers the inbound legacy user agent task handler to see if the incoming request is from a legacy agent.

Property name	<code>org.forgerock.agents.legacy.redirect.uri</code>
Deprecated in	5.6
Aliases	<code>com.sun.identity.agents.config.legacy.redirect.uri</code> Introduced in Java Agent 5.0 <u>Recognized</u> from AM 6 <code>org.forgerock.agents.legacy.redirect.uri</code> Introduced in Java Agent 5.6
Type	String
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>
AM console	Tab: Miscellaneous Title: Legacy User Agent Redirect URI

Legacy User Agent List (deprecated)

A list of legacy user agents.

Property name	<code>org.forgerock.agents.legacy.user.agent.list</code>
Deprecated in	5.6

Aliases	<p><code>com.sun.identity.agents.config.legacy.user.agent</code> Introduced in Java Agent 5.0 <u>Recognized</u> from AM 6</p> <p><code>org.forgerock.agents.legacy.user.agent.list</code> Introduced in Java Agent 5.6</p>
Type	List
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>
AM console	<p>Tab: Miscellaneous</p> <p>Title: Legacy User Agent List</p>

Locale

Locale Country

The agent country. Changing this has no effect.

Property name	<code>org.forgerock.agents.locale.country</code>
Aliases	<p><code>org.forgerock.agents.locale.country</code> Introduced in Java Agent 5.6</p> <p><code>com.sun.identity.agents.config.locale.country</code> Introduced in Java Agent 5.0 <u>Recognized</u> from AM 6</p>
Type	String
Default	US
Bootstrap property	No
Required property	No
Restart required	No

Local configuration file	AgentConfig.properties
AM console	Tab: Miscellaneous Title: Locale Country

Locale Language

The agent language. Changing this has no effect.

Property name	org.forgerock.agents.locale.language
Aliases	org.forgerock.agents.locale.language Introduced in Java Agent 5.6 com.sun.identity.agents.config.locale.language Introduced in Java Agent 5.0 <u>Recognized</u> from AM 6
Type	String
Default	en
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	AgentConfig.properties
AM console	Tab: Miscellaneous Title: Locale Language

Login

Enable Redirect to AM Success URL

When `true`, the agent redirects to the success URL specified in the AM service, if any. If no success URL is specified in AM, the agent redirects to the original requested URL, if any.

When `false`, the agent redirects to the requested URL, if any.

Property name	<code>org.forgerock.agents.authn.success.redirect.session.url.enabled</code>
Aliases	<code>org.forgerock.agents.authn.success.redirect.session.url.enabled</code> Introduced in Java Agent 5.6.3.0 <u>Recognized</u> from AM 7
Type	Boolean: true returns true; all other strings return false.
Default	false
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>
AM console	Tab: AM Services (from AM 7) Title: Enable Redirect to AM Success URL Legacy title: Redirect to AM's Success URL

Login Attempt Limit

When the value of this property is greater than zero, it defines the maximum number of failed login attempts allowed during a browser session. After this number, the agent blocks requests from the user.

Specify a value greater than zero. For example, if the property is set to 3, the agent blocks the fourth login request.

Use this property to mitigate the risk of brute force attacks.

Property name	<code>org.forgerock.agents.login.attempt.limit.count</code>
---------------	---

Aliases	<p><code>org.forgerock.agents.login.attempt.limit.count</code> Introduced in Java Agent 5.6</p> <p><code>com.sun.identity.agents.config.login.attempt.limit</code> Introduced in Java Agent 5.0 <u>Recognized</u> from AM 6</p>
Type	Integer
Default	0
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>
AM console	<p>Tab: Global</p> <p>Title: Login Attempt Limit</p>

Authentication Exchange Cookie Name

A cookie name that will be used by the authentication exchange endpoint. The value is empty by default, and the endpoint is not able to examine cookie values.

Property name	<code>org.forgerock.agents.authn.exchange.cookie.name</code>
Aliases	<p><code>org.forgerock.agents.authn.exchange.cookie.name</code> Introduced in Java Agent 5.7</p>
Type	String
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>
AM console	<p>Tab: SSO (from AM 7)</p> <p>Title: Authentication Exchange Cookie Name</p>

Login Attempt Limit Cookie Name

The name of the cookie used to record the number of login attempts.

Property name	<code>org.forgerock.agents.login.counter.cookie.name</code>
Aliases	<code>com.sun.identity.agents.config.login.counter.name</code> Introduced in Java Agent 5.0 <u>Recognized</u> from AM 7 <code>org.forgerock.agents.login.counter.cookie.name</code> Introduced in Java Agent 5.6
Type	String
Default	<code>amFilterParam</code>
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>
AM console	Tab: Global (from AM 7) Title: Login Attempt Limit Cookie Name

Login Reason Value Map

When Login Reason Parameter Name is set, this property specifies alternative strings to use for the supported values. For example:

Consider the example where Login Reason Parameter Name is set to `auth_reason`, and this property is set as follows:

```
org.forgerock.agents.login.reason.map[NO_TOKEN]=notoken
```

```
org.forgerock.agents.login.reason.map[TOKEN_EXPIRED]=expired
```

```
org.forgerock.agents.login.reason.map[EXCEPTION]=exception
```

The agent redirects authentication to the following URL:

https://custom.example.com:8443/.../login_endpoint?...&auth_reason=notoken&...

Property name	<code>org.forgerock.agents.login.reason.remapper</code>
Aliases	<code>org.forgerock.agents.login.reason.remapper</code> Introduced in Java Agent 5.7 <code>org.forgerock.agents.login.reason.map</code> Introduced in Java Agent 5.7 <u>Recognized</u> from AM 7
Type	Map <ul style="list-style-type: none">• Keys: failed login reason code• Values: masked value
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>
AM console	Tab: Miscellaneous (from AM 7) Title: Login Reason Value Map

Redirect Attempt Limit

When the value of this property is greater than zero, it defines the maximum number of redirects allowed for a browser session. After this number, the agent blocks the request.

Specify a value greater than zero. For example, if the property is set to 3, then the agent blocks the request on the fourth redirect.

Use this property to mitigate the risk of infinite redirection loops.

Property name	<code>org.forgerock.agents.redirect.attempt.limit</code>
---------------	--

Aliases	<p><code>org.forgerock.agents.redirect.attempt.limit</code> Introduced in Java Agent 5.6</p> <p><code>com.sun.identity.agents.config.redirect.attempt.limit</code> Introduced in Java Agent 5.0 <u>Recognized</u> from AM 6</p>
Type	Integer
Default	0
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	AgentConfig.properties
AM console	<p>Tab: Global</p> <p>Title: Redirect Attempt Limit</p>

Authentication Exchange URI

This property allows the administrator to enable an endpoint to facilitate the exchange of SSO tokens for OIDC JWTs. The value is empty by default and thus the endpoint is not accessible.

Property name	<code>org.forgerock.agents.authn.exchange.uri</code>
Aliases	<p><code>org.forgerock.agents.authn.exchange.uri</code> Introduced in Java Agent 5.7 <u>Recognized</u> from AM 7</p>
Type	String
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	AgentConfig.properties

AM console	Tab: SSO (from AM 7) Title: Authentication Exchange URI
------------	--

Login Redirect (Default)

OAuth Login URL List

Use only when Enable Custom Login Mode is `false` and AM Login URL List is empty.

Specify rules to evaluate the incoming request URL, based on domain, path, request header, or query parameters. Specify a URL for login redirect with optional parameters.

Format, with no spaces between values:

```
[domain/path][header:value][?param=value[, param=value]]|[URL][?param=value&param=value]
```

When an unauthenticated request URL matches a rule specified by this property, the agent redirects the request to the specified URL for login.

When this property configures multiple rules, the agent sorts the rules into the following order and applies them in that order until it finds a match:

1. Header specification - a rule with a header specification is applied before other rules
2. Longest domain
3. Longest path
4. Highest number of parameter specifications

During redirect, the agent appends the goto parameter configured in Goto Parameter Name, and a nonce parameter, to the agent's CDSSO endpoint. If Enable FQDN Checking is `true`, the agent iterates through the list of URLs until it finds a redirect URL that matches the FQDN check values. Otherwise, the agent redirects the user to the URL configured in the conditional redirect rules.

[domain/path]

The incoming request URL:

- Domain: For example, `example.com`. The agent must match the domain and its subdomains. For example, `example.com` matches `mydomain.example.com` and `www.example.com`. Domains can also include path information, for example, `example.com/market`, but cannot specify ports.
- Subdomain: For example, `mydomain.example.com`. The agent match the domain, the subdomain, and any sub-subdomain. For example, `mydomain.example.com`

matches `true.mydomain.example.com`. Subdomains can include path information, for example, `mydomain.example.com/s6ecure`, but cannot specify ports.

- Path: For example, `/myapp`.
- No value: Nothing is specified before the `|` character and the rule applies to every incoming request.

[header:value]

One header/value pair provided in the incoming request. If the header value is not provided, the header can take any value. For example:

Requests containing a header called `X-local` with the value provided are redirected to the default URL:

```
org.forgerock.agents.oauth.login.url.list[0]= X-local:provided|
```

Requests containing a header called `X-local` with any value are redirected to the default URL:

```
org.forgerock.agents.oauth.login.url.list[0]= X-local:|
```

[?param=value[,param=value]

One or more parameter and value pairs provided in the incoming request. If the parameter value is not provided, the parameter can take any value. For example:

Requests containing a parameter called `site` with the value `shopping` are redirected to the default URL:

```
org.forgerock.agents.oauth.login.url.list[2]= ?site=shopping|
```

Requests containing a parameter called `target`` with the value ``cooking` **AND** a parameter called `price` with the value `low` are redirected to the default URL:+

```
org.forgerock.openam.agents.config.conditional.login.url[0]= ?  
target=cooking,price=low|
```

[URL]

The login URL. The URL can be an AM instance, an AM site, or a website other than AM.

Specify a URL in the format `protocol://FQDN[:port]/URI`, where the port is optional if it is 80 or 443. For example:

```
https://myweb.example.com/authApp/login.jsp
```

```
https://am.example.com:8443/openam/XUI/#login/
```

```
https://am.example.com:8443/openam/customlogin/login.jsp
```

If [URL] is not specified, the agent redirects the request to the AM instance or site specified by the following bootstrap properties:

```
org.forgerock.agents.am.protocol://org.forgerock.agents.am.hostname:org.forgerock.agents.am.port/org.forgerock.agents.am.path
```

[?param=value¶m=value]

One or more parameters to add to the login URL. Chain multiple parameters with an ampersand (&), for example, realm=value¶meter1=value1¶meter2=value2 .

When the parameter is ?realm=value it specifies the AM realm into which the agent logs the users. For example, ?realm=marketplace .

When redirecting to AM's XUI, use an ampersand (&) instead of a question mark (?). For example,

```
https://am.example.com:8443/openam/XUI/#login/&realm=marketplace .
```

A realm parameter is not required in the login URL when any of the following conditions are true:

- The custom login page itself sets the realm parameter, for example, because it lets the user choose it. In this case, you must ensure the custom login page always returns a realm parameter to the agent.
- The realm that the agent is logging the user into has DNS aliases configured in AM.
- AM logs the user into the realm whose DNS alias matches the incoming request URL. For example, an inbound request from the http://marketplace.example.com URL logs in the marketplace realm if the realm alias is set to marketplace.example.com.
- The users should always log in to the Top Level Realm.

Examples

+

Requests containing a header called X-local with the value provided are redirected to the specified URL in the beta realm:

+

```
org.forgerock.agents.oauth.login.url.list[0]= X-local:provided|http://mysite.local.com:8081/login?realm=beta
```

+

Requests containing a header called X-local with any value are redirected to the default URL in the gamma realm:

+

`org.forgerock.agents.oauth.login.url.list[1]= X-local:|?realm=gamma`

+

Requests containing a parameter called `site` with the value `shopping` **AND** a parameter called `mode` with the value `discount` are redirected to the default URL in the `discountshopping` realm:

+

`org.forgerock.agents.oauth.login.url.list[2]= ?site=shopping,mode=discount|?realm=discountshopping`

+

Requests containing a parameter called `target` with the value `cooking` are redirected to the AM XUI page in the `kitchen` realm. Note the use of `&` before the realm parameter:

+

`org.forgerock.openam.agents.config.conditional.login.url[0]= ?target=cooking|https://am.example.com:8443/openam/XUI/#login/&realm=kitchen`

+

Requests containing a parameter called `target` with the value `cooking` are redirected to a non-AM login page in the `kitchen` realm. Note the use of `?` before the realm parameter:

+

`org.forgerock.openam.agents.config.conditional.login.url[0]= ?target=cooking|https://mysite.example.com:8443/login/?realm=kitchen`

Property name	<code>org.forgerock.agents.oauth.login.url.list</code>
Aliases	<code>org.forgerock.agents.oauth.login.url.list</code> Introduced in Java Agent 5.6 <code>org.forgerock.openam.agents.config.conditional.login.url</code> Introduced in Java Agent 5.6 <u>Recognized from AM 6</u>
Type	List
Bootstrap property	No

Required property	No
Restart required	No
Local configuration file	AgentConfig.properties
AM console	Tab: AM Services Title: OAuth Login URL List Legacy title: AM Conditional Login URL

Enable Custom Login Mode

Set the login redirection mode, as follows:

- `false` : Use default login redirection mode.
 - The agent can redirect requests to any AM instance that supports the `/oauth2/authorize` endpoint. By default, this is the AM instance that is specified during installation.
 - The `/oauth2/authorize` endpoint returns an OIDC ID token. This is the only response the agent accepts.
 - Use with [OAuth Login URL List](#) to modify or redirect calls to the endpoint that provides the tokens.
- `true` : Use custom login redirection mode.
 - The agent handles JWTs or SSO tokens as session tokens for authentication and authorization, and can can redirect login anywhere.
 - Use with [AM Login URL List](#) and [Legacy Login URL List](#) to modify or redirect calls.

During session upgrade, the format of the composite advice is as follows:

- When both this property and [Enable SSO Token Acceptance](#) are `true` , the composite advice has the following format: ?
authIndexType=composite_advice&authIndexValue=<Advices Value>
- When either property is `false` , the composite advice has the following format: ?
composite_advice=<Advices Value>

Property name	<code>org.forgerock.agents.legacy.login.enabled</code>
---------------	--

Aliases	<p><code>org.forgerock.agents.legacy.login.enabled</code> Introduced in Java Agent 5.6</p> <p><code>org.forgerock.openam.agents.config.allow.custom.login</code> Introduced in Java Agent 5.6 <u>Recognized</u> from AM 7</p>
Type	Boolean: true returns true; all other strings return false.
Default	false
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>
AM console	<p>Tab: AM Services (from AM 7)</p> <p>Title: Enable Custom Login Mode</p> <p>Legacy title: Allow Custom Login Mode</p>

AM Login URL List

The URL of the login page to use for authentication.

During the redirect, the agent appends the following parameters to the agent's CDSSO endpoint:

- The goto parameter configured in Goto Parameter Name
- A nonce parameter

Use the format `URL[?realm=realm_name?parameter1=value1&...]`, where:

- `URL` : URL of the login page to use for authentication
- `[?realm=realm_name¶meter1=value1&...]` : Optional parameters that the agent passes to the login page, for example, the AM realm at which to authenticate.

You do not need to specify an authentication realm if any of the following conditions are true:

- The custom login page sets the realm parameter, for example, because it lets the user choose the realm.
- The user authenticates into a realm that has DNS aliases configured in AM. AM then logs the user into the realm whose DNS alias matches the incoming request URL. For example, an inbound request from `http://marketplace.example.com` logs in the marketplace realm if the realm alias is set to `marketplace.example.com`.
- The user authenticates to the top-level realm.

This parameter can be overwritten by the custom login page if, for example, the user chooses the authentication realm.

Specify as many parameters your custom login pages require.

Example:

```
https://login.example.com/login.jsp?realm=marketplace&param1=value1
```

In some versions of AM you can configure more than one value for this property, but only the first value is honored.

Property name	<code>com.sun.identity.agents.config.login.url</code>
Aliases	<code>com.sun.identity.agents.config.login.url</code> Introduced in Java Agent 5.0 <u>Recognized</u> from AM 6
Type	List
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>
AM console	Tab: AM Services Title: AM Login URL List Legacy title: AM Login URL

Legacy Login URL List

Adds parameters conditionally to legacy login URLs.

Format, with no spaces between values:

```
domain/path|url?param1=value1&param2=value2
```

Domain/path

The incoming request URL:

- Domain: For example, `example.com`. The agent must match the domain and its subdomains. For example, `example.com` matches `mydomain.example.com` and `www.example.com`. Domains can also include path information, for example, `example.com/market`, but cannot specify ports.
- Subdomain: For example, `mydomain.example.com`. The agent match the domain, the subdomain, and any sub-subdomain. For example, `mydomain.example.com` matches `true.mydomain.example.com`. Subdomains can include path information, for example, `mydomain.example.com/s6ecure`, but cannot specify ports.
- Path: For example, `/myapp`.
- No value: Nothing is specified before the `|` character and the rule applies to every incoming request.

URL

The URL to which redirect incoming login requests. The URL may be an AM instance, an AM site, or a website other than AM.

Specify a URL in the format `protocol://FQDN[:port]/URI`, where the port is optional if it is 80 or 443. For example:

```
https://myweb.example.com/authApp/login.jsp
```

```
https://am.example.com:8443/openam/XUI/#login/
```

```
https://am.example.com:8443/openam/customlogin/login.jsp
```

If the URL is not specified, the agent redirects the request to the AM instance or site specified by the following bootstrap properties:

```
org.forgerock.agents.am.protocol://org.forgerock.agents.am.hostname:org.f  
orgerock.agents.am.port/org.forgerock.agents.am.path
```

¶meter1=value1

Parameters that can be added to the URL. Add as many parameters as your custom login pages need. Chain parameters with an `&` character, for example, `realm=value¶meter1=value1¶meter2=value2`.

Examples

```
org.forgerock.agents.legacy.login.url.list[0]=example.com|https://am.example  
.com/openam/XUI/#login&realm=customers
```

org.forgerock.agents.legacy.login.url.list[1]=myapp.domain.com|https://login.example.com/apps/login.jsp?realm=sales

org.forgerock.agents.legacy.login.url.list[2]=sales.example.com/marketplace|?realm=marketplace

org.forgerock.agents.legacy.login.url.list[3]=|https://login.example.com/apps/login.jsp?realm=sales&isblue=true&carowner=true

org.forgerock.agents.legacy.login.url.list[4]=|?realm=sales

Property name	org.forgerock.agents.legacy.login.url.list
Aliases	org.forgerock.openam.agents.config.conditional.custom.login.url Introduced in Java Agent 5.6 <u>Recognized</u> from AM 7 org.forgerock.agents.legacy.login.url.list Introduced in Java Agent 5.6
Type	List
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	AgentConfig.properties
AM console	Tab: AM Services (from AM 7) Title: Legacy Login URL List Legacy title: Custom Conditional Login URL

Login redirect

Enable SSO Token Acceptance

Set this property as follows:

- `true` : Accept SSO tokens. Use this option when the agent and the token issuer are in the same domain, and for web applications and APIs where the backend accepts user information from SSO tokens.

- `false` : Do not accept SSO tokens; require OIDC JWTs for authentication.

During session upgrade the format of the composite advice is as follows:

- When both this property and Enable Custom Login Mode are `true` , the composite advice has the following format: ?
`authIndexType=composite_advice&authIndexValue=<Advices Value>`
- When either property is `false` , the composite advice has the following format: ?
`composite_advice=<Advices Value>`

Property name	<code>org.forgerock.agents.accept.sso.tokens.enabled</code>
Aliases	<code>org.forgerock.agents.accept.sso.tokens.enabled</code> Introduced in Java Agent 5.7.1 <u>Recognized</u> from AM 7.1 <code>org.forgerock.agents.accept.sso.tokens</code> Introduced in Java Agent 5.7.1 <code>com.forgerock.agents.accept.sso.tokens</code> Introduced in Java Agent 5.7.1
Type	Boolean: <code>true</code> returns true; all other strings return <code>false</code> .
Default	<code>false</code>
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>
AM console	Tab: SSO (from AM 7.1) Title: Enable SSO Token Acceptance Legacy title: Accept SSO Tokens

OAuth Login URL List

Use only when Enable Custom Login Mode is `false` and AM Login URL List is empty.

Specify rules to evaluate the incoming request URL, based on domain, path, request header, or query parameters. Specify a URL for login redirect with optional parameters.

Format, with no spaces between values:

```
[domain/path][header:value][?param=value[, param=value]]|[URL][?param=value&param=value]
```

When an unauthenticated request URL matches a rule specified by this property, the agent redirects the request to the specified URL for login.

When this property configures multiple rules, the agent sorts the rules into the following order and applies them in that order until it finds a match:

1. Header specification - a rule with a header specification is applied before other rules
2. Longest domain
3. Longest path
4. Highest number of parameter specifications

During redirect, the agent appends the goto parameter configured in [Goto Parameter Name](#), and a nonce parameter, to the agent's CDSSO endpoint. If [Enable FQDN Checking](#) is `true`, the agent iterates through the list of URLs until it finds a redirect URL that matches the FQDN check values. Otherwise, the agent redirects the user to the URL configured in the conditional redirect rules.

[domain/path]

The incoming request URL:

- Domain: For example, `example.com`. The agent must match the domain and its subdomains. For example, `example.com` matches `mydomain.example.com` and `www.example.com`. Domains can also include path information, for example, `example.com/market`, but cannot specify ports.
- Subdomain: For example, `mydomain.example.com`. The agent match the domain, the subdomain, and any sub-subdomain. For example, `mydomain.example.com` matches `true.mydomain.example.com`. Subdomains can include path information, for example, `mydomain.example.com/s6ecure`, but cannot specify ports.
- Path: For example, `/myapp`.
- No value: Nothing is specified before the `|` character and the rule applies to every incoming request.

[header:value]

One header/value pair provided in the incoming request. If the header value is not provided, the header can take any value. For example:

Requests containing a header called `X-local` with the value provided are redirected to the default URL:

```
org.forgerock.agents.oauth.login.url.list[0]= X-local:provided|
```

Requests containing a header called `X-local` with any value are redirected to the default URL:

```
org.forgerock.agents.oauth.login.url.list[0]= X-local:|
```

[?param=value[, param=value]

One or more parameter and value pairs provided in the incoming request. If the parameter value is not provided, the parameter can take any value. For example:

Requests containing a parameter called `site` with the value `shopping` are redirected to the default URL:

```
org.forgerock.agents.oauth.login.url.list[2]= ?site=shopping|
```

Requests containing a parameter called `target` with the value `cooking` **AND** a parameter called `price` with the value `low` are redirected to the default URL:+

```
org.forgerock.openam.agents.config.conditional.login.url[0]= ?  
target=cooking,price=low|
```

[URL]

The login URL. The URL can be an AM instance, an AM site, or a website other than AM.

Specify a URL in the format `protocol://FQDN[:port]/URI`, where the port is optional if it is 80 or 443. For example:

```
https://myweb.example.com/authApp/login.jsp
```

```
https://am.example.com:8443/openam/XUI/#login/
```

```
https://am.example.com:8443/openam/customlogin/login.jsp
```

If `[URL]` is not specified, the agent redirects the request to the AM instance or site specified by the following bootstrap properties:

```
org.forgerock.agents.am.protocol://org.forgerock.agents.am.hostname:org.forg  
erock.agents.am.port/org.forgerock.agents.am.path
```

[?param=value¶m=value]

One or more parameters to add to the login URL. Chain multiple parameters with an ampersand (&), for example, `realm=value¶meter1=value1¶meter2=value2`.

When the parameter is `?realm=value` it specifies the AM realm into which the agent logs the users. For example, `?realm=marketplace`.

When redirecting to AM's XUI, use an ampersand (&) instead of a question mark (?). For example,

```
https://am.example.com:8443/openam/XUI/#login/&realm=marketplace .
```

A realm parameter is not required in the login URL when any of the following conditions are true:

- The custom login page itself sets the realm parameter, for example, because it lets the user choose it. In this case, you must ensure the custom login page always returns a realm parameter to the agent.
- The realm that the agent is logging the user into has DNS aliases configured in AM.
- AM logs the user into the realm whose DNS alias matches the incoming request URL. For example, an inbound request from the `http://marketplace.example.com` URL logs in the marketplace realm if the realm alias is set to `marketplace.example.com`.
- The users should always log in to the Top Level Realm.

Examples

+

Requests containing a header called `X-local` with the value `provided` are redirected to the specified URL in the `beta` realm:

+

```
org.forgerock.agents.oauth.login.url.list[0]= X-  
local:provided|http://mysite.local.com:8081/login?realm=beta
```

+

Requests containing a header called `X-local` with any value are redirected to the default URL in the `gamma` realm:

+

```
org.forgerock.agents.oauth.login.url.list[1]= X-local:|?realm=gamma
```

+

Requests containing a parameter called `site` with the value `shopping` **AND** a parameter called `mode` with the value `discount` are redirected to the default URL in the `discountshopping` realm:

+

```
org.forgerock.agents.oauth.login.url.list[2]= ?site=shopping,mode=discount|?  
realm=discountshopping
```

+

Requests containing a parameter called `target` with the value `cooking` are redirected to the AM XUI page in the `kitchen` realm. Note the use of `&` before the realm parameter:

+

```
org.forgerock.openam.agents.config.conditional.login.url[0]= ?
target=cooking|https://am.example.com:8443/openam/XUI/#login/&realm=kitchen
```

+

Requests containing a parameter called `target` with the value `cooking` are redirected to a non-AM login page in the `kitchen` realm. Note the use of `?` before the realm parameter:

+

```
org.forgerock.openam.agents.config.conditional.login.url[0]= ?
target=cooking|https://mysite.example.com:8443/login/?realm=kitchen
```

Property name	<code>org.forgerock.agents.oauth.login.url.list</code>
Aliases	<code>org.forgerock.agents.oauth.login.url.list</code> Introduced in Java Agent 5.6 <code>org.forgerock.openam.agents.config.conditional.login.url</code> Introduced in Java Agent 5.6 <u>Recognized</u> from AM 6
Type	List
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>
AM console	Tab: AM Services Title: OAuth Login URL List Legacy title: AM Conditional Login URL

Enable Custom Login Mode

Set the login redirection mode, as follows:

- `false` : Use default login redirection mode.
 - The agent can redirect requests to any AM instance that supports the `/oauth2/authorize` endpoint. By default, this is the AM instance that is specified during installation.
 - The `/oauth2/authorize` endpoint returns an OIDC ID token. This is the only response the agent accepts.
 - Use with [OAuth Login URL List](#) to modify or redirect calls to the endpoint that provides the tokens.
- `true` : Use custom login redirection mode.
 - The agent handles JWTs or SSO tokens as session tokens for authentication and authorization, and can can redirect login anywhere.
 - Use with [AM Login URL List](#) and [Legacy Login URL List](#) to modify or redirect calls.

During session upgrade, the format of the composite advice is as follows:

- When both this property and [Enable SSO Token Acceptance](#) are `true` , the composite advice has the following format: ?
`authIndexType=composite_advice&authIndexValue=<Advices Value>`
- When either property is `false` , the composite advice has the following format: ?
`composite_advice=<Advices Value>`

Property name	<code>org.forgerock.agents.legacy.login.enabled</code>
Aliases	<code>org.forgerock.agents.legacy.login.enabled</code> Introduced in Java Agent 5.6 <code>org.forgerock.openam.agents.config.allow.custom.login</code> Introduced in Java Agent 5.6 Recognized from AM 7
Type	Boolean: <code>true</code> returns true; all other strings return <code>false</code> .
Default	<code>false</code>
Bootstrap property	No
Required property	No
Restart required	No

Local configuration file	AgentConfig.properties
AM console	Tab: AM Services (from AM 7) Title: Enable Custom Login Mode Legacy title: Allow Custom Login Mode

AM Login URL List

The URL of the login page to use for authentication.

During the redirect, the agent appends the following parameters to the agent's CDSSO endpoint:

- The goto parameter configured in [Goto Parameter Name](#)
- A nonce parameter

Use the format `URL[?realm=realm_name?parameter1=value1&...]` , where:

- URL : URL of the login page to use for authentication
- `[?realm=realm_name¶meter1=value1&...]` : Optional parameters that the agent passes to the login page, for example, the AM realm at which to authenticate.

You do not need to specify an authentication realm if any of the following conditions are true:

- The custom login page sets the realm parameter, for example, because it lets the user choose the realm.
- The user authenticates into a realm that has DNS aliases configured in AM. AM then logs the user into the realm whose DNS alias matches the incoming request URL. For example, an inbound request from `http://marketplace.example.com` logs in the marketplace realm if the realm alias is set to `marketplace.example.com`.
- The user authenticates to the top-level realm.

This parameter can be overwritten by the custom login page if, for example, the user chooses the authentication realm.

Specify as many parameters your custom login pages require.

Example:

```
https://login.example.com/login.jsp?realm=marketplace&param1=value1
```

In some versions of AM you can configure more than one value for this property, but only the first value is honored.

Property name	<code>com.sun.identity.agents.config.login.url</code>
Aliases	<code>com.sun.identity.agents.config.login.url</code> Introduced in Java Agent 5.0 <u>Recognized</u> from AM 6
Type	List
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>
AM console	Tab: AM Services Title: AM Login URL List Legacy title: AM Login URL

Login Reason Parameter Name

When Enable Custom Login Mode is `true`, this property specifies the name of a parameter included in calls to the custom login URL, to indicate why authentication is required. The parameter value can be used in a custom login page to provide additional feedback to the authenticating user.

If this property is specified, the agent includes a parameter named with the property value, and including one of the following values:

- `NO_TOKEN`: No token present in the original request.
- `TOKEN_EXPIRED`: Expiry time of the JWT was in the past.
- `EXCEPTION`: An unknown exception occurred, either while parsing the JWT or at some other stage of authentication.

To reduce the risk of leaking useful information, use the property Login Reason Value Map to change the strings for the above values.

For example, specifying

`org.forgerock.agents.login.reason.parameter.name=auth_reason` can cause the agent to redirect authentication to the following URL:

https://custom.example.com:8443/.../login_endpoint?...
&auth_reason=TOKEN_EXPIRED&...

Do not enter a value that clashes with other parameters used for authentication; for example, realm or goto.

Property name	org.forgerock.agents.login.reason.parameter.name
Aliases	org.forgerock.agents.login.reason.parameter.name Introduced in Java Agent 5.7
Type	String
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	AgentConfig.properties
AM console	Tab: Miscellaneous (from AM 7) Title: Login Reason Parameter Name

Legacy Login URL List

Adds parameters conditionally to legacy login URLs.

Format, with no spaces between values:

domain/path|url?param1=value1¶m2=value2

Domain/path

The incoming request URL:

- Domain: For example, example.com. The agent must match the domain and its subdomains. For example, example.com matches mydomain.example.com and www.example.com. Domains can also include path information, for example, example.com/market, but cannot specify ports.
- Subdomain: For example, mydomain.example.com. The agent match the domain, the subdomain, and any sub-subdomain. For example, mydomain.example.com matches true.mydomain.example.com. Subdomains can include path information, for example, mydomain.example.com/secure, but cannot specify ports.
- Path: For example, /myapp.

- No value: Nothing is specified before the | character and the rule applies to every incoming request.

URL

The URL to which redirect incoming login requests. The URL may be an AM instance, an AM site, or a website other than AM.

Specify a URL in the format `protocol://FQDN[:port]/URI`, where the port is optional if it is 80 or 443. For example:

```
https://myweb.example.com/authApp/login.jsp
```

```
https://am.example.com:8443/openam/XUI/#login/
```

```
https://am.example.com:8443/openam/customlogin/login.jsp
```

If the URL is not specified, the agent redirects the request to the AM instance or site specified by the following bootstrap properties:

```
org.forgerock.agents.am.protocol://org.forgerock.agents.am.hostname:org.f
orgerock.agents.am.port/org.forgerock.agents.am.path
```

¶meter1=value1

Parameters that can be added to the URL. Add as many parameters as your custom login pages need. Chain parameters with an & character, for example, `realm=value¶meter1=value1¶meter2=value2`.

Examples

```
org.forgerock.agents.legacy.login.url.list[0]=example.com|https://am.example
.com/openam/XUI/#login&realm=customers
```

```
org.forgerock.agents.legacy.login.url.list[1]=myapp.domain.com|https://login
.example.com/apps/login.jsp?realm=sales
```

```
org.forgerock.agents.legacy.login.url.list[2]=sales.example.com/marketplace|
?realm=marketplace
```

```
org.forgerock.agents.legacy.login.url.list[3]=|https://login.example.com/app
s/login.jsp?realm=sales&isblue=true&carowner=true
```

```
org.forgerock.agents.legacy.login.url.list[4]=|?realm=sales
```

Property name	<code>org.forgerock.agents.legacy.login.url.list</code>
---------------	---

Aliases	<p><code>org.forgerock.openam.agents.config.conditional.custom.login.url</code> Introduced in Java Agent 5.6 <u>Recognized</u> from AM 7</p> <p><code>org.forgerock.agents.legacy.login.url.list</code> Introduced in Java Agent 5.6</p>
Type	List
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>
AM console	<p>Tab: AM Services (from AM 7)</p> <p>Title: Legacy Login URL List</p> <p>Legacy title: Custom Conditional Login URL</p>

Logout

Logout URI Map

A map of request URIs that trigger logout of the user session. Use the following key:value format:

```
web application name:logout URI
```

When a URL that includes the specified URI is invoked, the agent kills the current session. It invokes the AM REST logout endpoint or the endpoint configured by Conditional Logout URL List.

The agent must be able to access the context for the URL. When a web application is specified, it must exist and the agent must have access to it.

The URL is a dummy URL. Even if a resource exists at the URL, it is never accessed.

Although logout can be triggered within any web application by invoking a single, common, URI, you can tailor it for particular web applications:

- To specify a single, common, URI, leave the key empty.

- To specify a URI unique to a particular web application, specify the name of the web application as the key.

Property name	<code>org.forgerock.agents.logout.endpoint.map</code>
Aliases	<code>com.sun.identity.agents.config.logout.uri</code> Introduced in Java Agent 5.0 <u>Recognized</u> from AM 6 <code>org.forgerock.agents.logout.endpoint.map</code> Introduced in Java Agent 5.6
Type	Map <ul style="list-style-type: none"> • Keys: web application • Values: URI of dummy endpoint which will trigger logout
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>
AM console	Tab: Application Title: Logout URI Map Legacy title: Application Logout URI

Logout Request Parameter Map

A map of request parameters that trigger logout of the user session. Use the following key:value format:

``web application name:parameter name to trigger logout`

The agent searches every incoming request for the parameter. When the agent detects the parameter, it invokes AM to kill the current session for the specified web application or all web applications.

The request URL must contain the parameter, but does not need to assign a value to the parameter.

Although logout can be triggered within any web application by invoking a single, common, URI, you can tailor it for particular web applications:

- To specify a single, common, URI, leave the key empty.
- To specify a URI unique to a particular web application, specify the name of the web application as the key.

Property name	<code>org.forgerock.agents.logout.request.param.map</code>
Aliases	<code>org.forgerock.agents.logout.request.param.map</code> Introduced in Java Agent 5.6 <code>com.sun.identity.agents.config.logout.request.param</code> Introduced in Java Agent 5.0 <u>Recognized</u> from AM 6
Type	Map <ul style="list-style-type: none"> • Keys: web application • Values: (single) HTTP query parameter to trigger logout
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>
AM console	Tab: Application Title: Logout Request Parameter Map Legacy title: Logout Request Parameter

Always invalidate sessions

When `false`, the agent does not invoke the AM REST logout endpoint to kill the user session.

If Conditional Logout URL List is configured with a URL that does not perform a REST logout to AM, set this property to `true`. The agent additionally invokes the AM REST logout endpoint to invalidate the session.

Property name	<code>org.forgerock.agents.config.logout.session.invalidate.enabled</code>
Aliases	<code>org.forgerock.agents.config.logout.session.invalidate.enabled</code> Introduced in Java Agent 5.10.1 <code>org.forgerock.agents.config.logout.session.invalidate</code> Introduced in Java Agent 5.10.1
Type	Boolean: <code>true</code> returns true; all other strings return <code>false</code> .
Default	<code>true</code>
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>

Enable Logout Introspection

When `true`, the agent checks the HTTP request body to locate the value of [Logout Request Parameter Map](#).

Property name	<code>org.forgerock.agents.logout.introspection.enabled</code>
Aliases	<code>com.sun.identity.agents.config.logout.introspect.enabled</code> Introduced in Java Agent 5.0 Recognized from AM 6 <code>org.forgerock.agents.logout.introspection.enabled</code> Introduced in Java Agent 5.6
Type	Boolean: <code>true</code> returns true; all other strings return <code>false</code> .
Default	<code>false</code>

Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	AgentConfig.properties
AM console	Tab: Application Title: Enable Logout Introspection Legacy title: Logout Introspect Enabled

Conditional Logout URL List

Define URLs to which the agent can conditionally direct the user on logout. This property does not trigger logout.

If this property is configured with a URL that does not perform a REST logout to AM, set Always invalidate sessions to `true`. The agent additionally invokes the AM REST logout endpoint to invalidate the session.

Configure one or more conditions, using this format:

```
domain/path|url?param1=value1&param2=value2
```

The request URL is compared to each condition in the list until a match is found. Conditions are evaluated by order of length, starting with the longest, irrespective of their order in the list.

In the following example, `example.com/path` is evaluated before `example.com`; the default condition is the shortest, and is evaluated last:

```
org.forgerock.agents.conditional.logout.url.list[0]=example.com|?additional=value
```

```
org.forgerock.agents.conditional.logout.url.list[1]=example.com/path|?one=red&two=green&three=blue
```

```
org.forgerock.agents.conditional.logout.url.list[2]=mybank.com|http://mybank.com/myapp/logout?param=override
```

```
org.forgerock.agents.conditional.logout.url.list[3]=|?alpha=beta
```

Property name	<code>org.forgerock.agents.conditional.logout.url.list</code>
---------------	---

Aliases	<p><code>org.forgerock.openam.agents.config.conditional.logout.url</code> Introduced in Java Agent 5.6 <u>Recognized</u> from AM 6</p> <p><code>org.forgerock.agents.conditional.logout.url.list</code> Introduced in Java Agent 5.6</p>
Type	List
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>
AM console	<p>Tab: AM Services</p> <p>Title: Conditional Logout URL List</p> <p>Legacy title: AM Conditional Logout URL</p>

Logout Entry URI Map

After logout has been triggered by [Logout URI Map](#) or [Logout Request Parameter Map](#), and is complete, the agent redirects users to a specified resource, such as an HTML page or JSP file.

The specified resource is automatically added to the not-enforced list, so that it can be accessed without authentication.

To redirect for a specific web application, set the key to the name of the web application.

To redirect for all web applications, leave the key empty.

Property name	<code>org.forgerock.agents.logout.goto.map</code>
Aliases	<p><code>com.sun.identity.agents.config.logout.entry.uri</code> Introduced in Java Agent 5.0 <u>Recognized</u> from AM 6</p> <p><code>org.forgerock.agents.logout.goto.map</code> Introduced in Java Agent 5.6</p>

Type	Map <ul style="list-style-type: none"> • Keys: web application • Values: URI of page explaining the user has been logged out
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	AgentConfig.properties
AM console	Tab: Application Title: Logout Entry URI Map Legacy title: Logout Entry URI

Logs

Agent Debug Level

The agent log level.

Make sure your container captures messages written to the standard output. Some containers do not, and warnings or critical errors can disappear forever.

Property name	org.forgerock.agents.debug.level
Aliases	com.ipplanet.services.debug.level Introduced in Java Agent 5.0 <u>Recognized</u> from AM 6 org.forgerock.agents.debug.level Introduced in Java Agent 5.6

Supported settings	<p>OFF (Deprecated) Uses the same log level as <code>ERROR</code>. To disable logging, edit <code>agent-logback.xml</code>. Forgerock advises not to disable logging.</p> <p>ERROR Log only errors.</p> <p>WARNING Log errors and warnings.</p> <p>MESSAGE Log errors, warnings, and informative messages.</p> <p>DEBUG Log errors, warnings, informative messages, and some debugging messages.</p> <p>TRACE Log fine-grained information, when you need the full visibility of what is happening in your application. This log level can create big log files, so use only when necessary, and then reduce the log level.</p> <p>ON (Deprecated) Uses the same log level as <code>TRACE</code>. When the log level is <code>ON</code>, <code>TRACE</code> level logs are written to file. In previous releases, <code>TRACE</code> level logs were written to the standard output. Make sure your container captures messages written to the standard output.</p>
Default	ERROR
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>
AM console	<p>Tab: Global</p> <p>Title: Agent Debug Level</p>

Miscellaneous

Redirect Attempt Cookie Name

The cookie name to use to detect redirect loops while authenticating, which would indicate a cookie domain problem.

Property name	<code>org.forgerock.agents.redirect.cookie.name</code>
Aliases	<code>org.forgerock.agents.redirect.cookie.name</code> Introduced in Java Agent 5.6 <code>com.sun.identity.agents.config.redirect.cookie.name</code> Introduced in Java Agent 5.0 <u>Recognized</u> from AM 7
Type	String
Default	<code>amFilterRDParam</code>
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>
AM console	Tab: Global (from AM 7) Title: Redirect Attempt Cookie Name

Encrypted Agent Password

The agent profile password, which must correspond to the value in AM.

Set this property to the encrypted value of the password, where the password is encrypted using the key in the property Encryption Key/Salt.

Use the following command to get the encrypted value of the password, where `passwordFile` contains only the password followed by a newline, and has the access permission `400`:

```
$ ./agentadmin --encrypt agentInstance passwordFile
```

Default: Empty

Property name	<code>org.forgerock.agents.encrypted.password</code>
Aliases	<code>com.ipplanet.am.service.secret</code> Introduced in Java Agent 5.0 <code>org.forgerock.agents.encrypted.password</code> Introduced in Java Agent 5.6
Type	String
Bootstrap property	No
Required property	Yes - If this property is missing, the agent fails to start
Restart required	Yes - Restart the container after changing the property
Local configuration file	<code>AgentPassword.properties</code>

Enable Ignore Path Info

When `true`, when the request URL contains a wildcard '*' character, the path info and query are stripped from the URL before it is compared with the list of not-enforced URLs.

Property name	<code>org.forgerock.agents.ignore.path.info.enabled</code>
Aliases	<code>com.sun.identity.agents.config.ignore.path.info</code> Introduced in Java Agent 5.0 <u>Recognized</u> from AM 6 <code>org.forgerock.agents.ignore.path.info.enabled</code> Introduced in Java Agent 5.6
Type	Boolean: <code>true</code> returns true; all other strings return <code>false</code> .
Default	<code>false</code>
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>

AM console	Tab: Miscellaneous Title: Enable Ignore Path Info Legacy title: Ignore Path Info for Not Enforced URLs
------------	--

Custom Response Header Map

A key:value map of custom headers set by the agent for the client, where the key is the header name, and the value is the header value. For example,
`org.forgerock.agents.response.header.map[Cache-Control]=no-cache`

Format `org.forgerock.agents.response.header.map[HEADER-NAME]=HEADER-VALUE`

Property name	<code>org.forgerock.agents.response.header.map</code>
Aliases	<code>org.forgerock.agents.response.header.map</code> Introduced in Java Agent 5.6 <code>com.sun.identity.agents.config.response.header</code> Introduced in Java Agent 5.0 <u>Recognized</u> from AM 6
Type	Map <ul style="list-style-type: none"> • Keys: from header • Values: to header
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>
AM console	Tab: Global Title: Custom Response Header Map Legacy title: Custom Response Header

Idle Time Refresh Window

The interval in minutes at which the agent calls AM to refresh a session idle timeout.

AM sessions have an idle timeout after which they expire. In general, when users access protected resources through an agent, the agent requests a policy decision on behalf of that user, which resets the idle timeout.

When the agent does not need to contact AM frequently, for example, when policy evaluation is already cached, sessions may unexpectedly expire in AM before the user has finished accessing the application.

Agents make one call per active user session at the end of the time interval, provided that the user is actively accessing the web application or site. If the user does not access the application during the configured window interval time, the agent will not make the call to AM at the end of the interval. Eventually, if the user is inactive for enough time, AM will log them out when the session reaches its idle timeout.

Configuring the idle timeout window to a short value, such as one minute, achieves a good balance between making additional calls to AM and providing a good user experience.

Increase this value only if the performance impact of making an extra call to AM every minute is noticeable enough in your environment.

Property name	<code>org.forgerock.agents.idle.time.window.minutes</code>
Aliases	<code>org.forgerock.agents.idle.time.window.minutes</code> Introduced in Java Agent 5.6.2.1 <u>Recognized</u> from AM 7
Type	Integer
Default	1
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>
AM console	Tab: Advanced (from AM 7) Title: Idle Time Refresh Window

Service Resolver Class Name

The Java class name of the service resolver used to override the ForgeRock provided service resolver. Use this property to customize pre-handlers and post-handlers.

Property name	<code>org.forgerock.agents.service.resolver.class.name</code>
Aliases	<code>org.forgerock.agents.service.resolver.class.name</code> Introduced in Java Agent 5.6.2.1 <u>Recognized</u> from AM 7
Type	String
Default	<code>com.sun.identity.agents.arch.ServiceResolver</code>
Bootstrap property	Yes
Required property	No
Restart required	Yes - Restart the container after changing the property
Local configuration file	<code>AgentBootstrap.properties</code>

HTTP Session Binding

When `true`, the agent invalidates the HTTP session in these circumstances:

- Login failure
- When the user has no SSO session
- When the principal user name does not match the SSO user name

Property name	<code>org.forgerock.agents.http.session.binding.enabled</code>
Aliases	<code>com.sun.identity.agents.config.httpsession.binding</code> Introduced in Java Agent 5.0 <u>Recognized</u> from AM 6 <code>org.forgerock.agents.http.session.binding.enabled</code> Introduced in Java Agent 5.6
Type	Boolean: <code>true</code> returns true; all other strings return <code>false</code> .
Default	<code>true</code>

Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	AgentConfig.properties
AM console	Tab: Global Title: HTTP Session Binding

Public AM URL

The assembled "public" URL of AM. This URL is used by the agent to redirect the user's browser to AM for login (customised or not), or if necessary, exchange an SSO token for a JWT.

The following properties make up the URL:

- [AM Authentication Service Protocol](#)
- [AM Authentication Service Host Name](#)
- [AM Authentication Service Port](#)
- [AM Authentication Service Path](#)

The "private" URL is used by the agent for tasks such as establishing websockets, and obtaining authentication tokens or session information. The AM or load balancer instance can be behind a firewall to which the agent has access.

Define this property when public access to AM is restricted to a different URL from the private URL.

Property name	org.forgerock.agents.public.am.url
Aliases	com.forgerock.agents.public.am.url Introduced in Java Agent 5.6.3.0 org.forgerock.agents.public.am.url Introduced in Java Agent 5.6.3.0
Type	String
Bootstrap property	Yes
Required property	Yes - If this property is missing, the agent fails to start

Restart required	Yes - Restart the container after changing the property
Local configuration file	AgentBootstrap.properties

Monitoring

Export Monitoring Metrics to CSV

When `true`, enables the export of agent performance monitoring metrics to comma-separated value (CSV) files.

Files are written the same directory as the agent instance debug files, for example in `/path/to/java_agents/tomcat_agent/Agent_001/logs/debug/`.

Property name	<code>org.forgerock.agents.config.monitoring.to.csv</code>
Aliases	<code>org.forgerock.agents.config.monitoring.to.csv</code> Introduced in Java Agent 5.6 <u>Recognized</u> from AM 7 <code>org.forgerock.agents.monitoring.to.csv.enabled</code> Introduced in Java Agent 5.6
Type	Boolean: <code>true</code> returns true; all other strings return <code>false</code> .
Default	<code>false</code>
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>
AM console	Tab: Advanced (from AM 7) Title: Export Monitoring Metrics to CSV

CSV Monitoring Directory

The full path to the directory where the agent writes CSV monitoring files, when CSV monitoring is enabled.

The default is set by the installer and written to the bootstrap properties file.

Default: `/logs/debug` directory relative to the `definedBy` of the agent installation

Property name	<code>org.forgerock.agents.csv.monitoring.directory</code>
Aliases	<code>org.forgerock.agents.csv.monitoring.directory</code> Introduced in Java Agent 5.7
Type	String
Bootstrap property	Yes
Required property	No
Restart required	Yes - Restart the container after changing the property
Local configuration file	<code>AgentBootstrap.properties</code>

Not-enforced

Not-Enforced URIs

A space-delimited list of URIs for which the agent does not enforce authentication or request policy evaluations. In the following example, the agent does not enforce authentication or request policy evaluations for the `public` and `images` directories of `myapp.example.com`:

```
org.forgerock.agents.notenforced.uri.list=https://myapp.example.com:8443/public/* https://myapp.example.com:8443/images/*
```

For more information and examples, see [Conventions for not-enforced rules](#).

Property name	<code>org.forgerock.agents.notenforced.uri.list</code>
Aliases	<code>org.forgerock.agents.notenforced.uri.list</code> Introduced in Java Agent 5.6 <code>com.sun.identity.agents.config.notenforced.uri</code> Introduced in Java Agent 5.0 Recognized from AM 6

Type	List
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	AgentConfig.properties

Not-Enforced Client IP List

A space-delimited list of IP addresses or network CIDR notation addresses for which the agent does not enforce authentication or request policy evaluations.

Supported values are IPV4 and IPV6 addresses, IPV4 and IPV6 ranges of addresses delimited by the - character, and network ranges specified in CIDR notation.

Property name	<code>org.forgerock.agents.notenforced.ip.list</code>
Aliases	<code>org.forgerock.agents.notenforced.ip.list</code> Introduced in Java Agent 5.6 <code>com.sun.identity.agents.config.notenforced.ip</code> Introduced in Java Agent 5.0 <u>Recognized</u> from AM 6
Type	List
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	AgentConfig.properties

Not-Enforced Favicon

When `true`, the agent does not enforce access to any files named `favicon.ico`, by inserting an internal not-enforced rule of `GET */favicon.ico`.

Property name	<code>org.forgerock.agents.auto.not.enforce.favicon</code>
---------------	--

Aliases	<p><code>org.forgerock.agents.auto.not.enforce.favicon</code> Introduced in Java Agent 5.7 <u>Recognized</u> from AM 7</p> <p><code>org.forgerock.agents.auto.not.enforce.favicon.enabled</code> Introduced in Java Agent 5.7</p>
Type	Boolean: true returns true; all other strings return false.
Default	true
Bootstrap property	Yes
Required property	No
Restart required	Yes - Restart the container after changing the property
Local configuration file	<code>AgentBootstrap.properties</code>
AM console	<p>Tab: Application (from AM 7)</p> <p>Title: Not-Enforced Favicon</p> <p>Legacy title: Not Enforced Favicon</p>

Enable Not-Enforced URIs Cache

When `true`, the agent caches evaluations of the Not-Enforced URIs.

Enable this setting when configuring many rules.

Property name	<code>org.forgerock.agents.notenforced.uri.cache.enabled</code>
Aliases	<p><code>org.forgerock.agents.notenforced.uri.cache.enabled</code> Introduced in Java Agent 5.6</p> <p><code>com.sun.identity.agents.config.notenforced.uri.cache.enable</code> Introduced in Java Agent 5.0 <u>Recognized</u> from AM 6</p>

Type	Boolean: true returns true; all other strings return false .
Default	true
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	AgentConfig.properties
AM console	Tab: Application Title: Enable Not-Enforced URIs Cache Legacy title: Not Enforced URIs Cache Enabled

Container Character Encoding

The character encoding used by the agent when encoding extended characters in the resource paths of not-enforced rules.

Property name	org.forgerock.agents.container.encoding
Aliases	org.forgerock.agents.container.encoding Introduced in Java Agent 5.9.1
Type	String
Default	UTF-8
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	AgentConfig.properties

Java Class for Matching Not Enforced Rules

The Java class used to match URIs and IP addresses embedded within not enforced rules.

The specified class must implement the interface `com.sun.identity.agents.common.RulePatternMatcher`.

If the class fails to instantiate, an error is logged and the default `NotEnforcedRulePatternMatcher` is created instead.

Property name	<code>org.forgerock.agents.not.enforced.rule.pattern.matcher.classname</code>
Aliases	<code>org.forgerock.agents.not.enforced.rule.pattern.matcher.classname</code> Introduced in Java Agent 5.9.0
Type	String
Default	<code>com.sun.identity.agents.common.NotEnforcedRulePatternMatcher</code>
Bootstrap property	Yes
Required property	No
Restart required	No
Local configuration file	<code>AgentBootstrap.properties</code>

Not-Enforced Compound Rule Separator

A delimiter for not-enforced compound rules. The delimiter can be a single character or a string. For example, setting the delimiter to `&&` allows compound rules to be specified as:

```
GET 10.5.1.5 100.2.21.36 && /public/*
```

```
REGEX 10\.4\.3\.5 && [^/]+\./free.jpg
```

Property name	<code>org.forgerock.agents.notenforced.compound.separator</code>
Aliases	<code>org.forgerock.agents.notenforced.compound.separator</code> Introduced in Java Agent 5.6 <code>com.sun.identity.agents.config.notenforced.rule.compound.separator</code> Introduced in Java Agent 5.0 <u>Recognized</u> from AM 7

Type	String
Default	
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	AgentConfig.properties
AM console	Tab: Application Title: Not-Enforced Compound Rule Separator

Invert Not-Enforced URIs

NOTE

The use of this property is NOT recommended.

When `true`, enforce policy for the URIs and patterns specified by the [Not-Enforced URIs](#) property, instead of allowing access to them without authentication.

For security considerations, do not enable this property. Instead, ForgeRock recommends using the NOT keyword to invert specific rules in the [Not-Enforced URIs](#).

Property name	<code>org.forgerock.agents.notenforced.uri.invert.enabled</code>
Aliases	<code>com.sun.identity.agents.config.notenforced.uri.invert</code> Introduced in Java Agent 5.0 <u>Recognized</u> from AM 6 <code>org.forgerock.agents.notenforced.uri.invert.enabled</code> Introduced in Java Agent 5.6
Type	Boolean: <code>true</code> returns true; all other strings return <code>false</code> .
Default	<code>false</code>
Bootstrap property	No

Required property	No
Restart required	No
Local configuration file	AgentConfig.properties
AM console	Tab: Application Title: Invert Not-Enforced URIs Legacy title: Invert Not Enforced URIs

Max Entries in Not-Enforced URI Cache

The maximum number of cached resource URLs that are matched by a not-enforced rule (inverted or not inverted).

Property name	<code>org.forgerock.agents.notenforced.uri.cache.size</code>
Aliases	<code>com.sun.identity.agents.config.notenforced.uri.cache.size</code> Introduced in Java Agent 5.0 <u>Recognized</u> from AM 6 <code>org.forgerock.agents.notenforced.uri.cache.size</code> Introduced in Java Agent 5.6
Type	Integer
Default	10000
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	AgentConfig.properties
AM console	Tab: Application Title: Max Entries in Not-Enforced URI Cache Legacy title: Not Enforced URIs Cache Size

Enable Not-Enforced IP Cache

NOTE

The use of this property is NOT recommended.

When `true`, the agent caches evaluations of the [Not-Enforced Client IP List](#).

Enable this setting if you are configuring many rules.

Property name	<code>org.forgerock.agents.notenforced.ip.cache.enabled</code>
Aliases	<code>org.forgerock.agents.notenforced.ip.cache.enabled</code> Introduced in Java Agent 5.6 <code>com.sun.identity.agents.config.notenforced.ip.cache.enabled</code> Introduced in Java Agent 5.0 Recognized from AM 6
Type	Boolean: <code>true</code> returns true; all other strings return false.
Default	<code>true</code>
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>
AM console	Tab: Application Title: Enable Not-Enforced IP Cache Legacy title: Not Enforced IP Cache Flag

Invert Not-Enforced IPs

When `true`, enforce policy for the IPs specified by the [Not-Enforced Client IP List](#) property, instead of allowing access to them without authentication.

For security considerations, do not enable this property. Instead, ForgeRock recommends using the NOT keyword to invert specific rules in the [Not-Enforced Client IP List](#).

Property name	<code>org.forgerock.agents.notenforced.ip.invert.enabled</code>
Aliases	<code>org.forgerock.agents.notenforced.ip.invert.enabled</code> Introduced in Java Agent 5.6 <code>com.sun.identity.agents.config.notenforced.ip.invert</code> Introduced in Java Agent 5.0 Recognized from AM 6
Type	Boolean: true returns true; all other strings return false.
Default	false
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>
AM console	Tab: Application Title: Invert Not-Enforced IPs Legacy title: Invert Not Enforced IPs

Max Entries in Not-Enforced IP Cache

The maximum number of cached IP addresses that are matched by a not-enforced rule (inverted or not inverted).

Property name	<code>org.forgerock.agents.notenforced.ip.cache.size</code>
---------------	---

Aliases	<p><code>org.forgerock.agents.notenforced.ip.cache.size</code> Introduced in Java Agent 5.6</p> <p><code>com.sun.identity.agents.config.notenforced.ip.cache.size</code> Introduced in Java Agent 5.0 <u>Recognized</u> from AM 6</p>
Type	Integer
Default	1000
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	AgentConfig.properties
AM console	<p>Tab: Application</p> <p>Title: Max Entries in Not-Enforced IP Cache</p> <p>Legacy title: Not Enforced IP Cache Size</p>

Container Parameter Encoding

The character encoding used by the agent when encoding extended characters in the HTTP query parameters of not-enforced rules.

Property name	<code>org.forgerock.agents.container.param.encoding</code>
Aliases	<p><code>org.forgerock.agents.container.param.encoding</code> Introduced in Java Agent 5.9.1</p>
Type	String
Default	ISO-8859-1
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	AgentConfig.properties

Notifications

Enable Notifications of Agent Configuration Change

Flag to indicate whether the agent subscribes to WebSocket notifications from AM for configuration changes. This property applies only the agent profile is stored in AM's configuration data store.

Property name	<code>org.forgerock.agents.config.change.notifications.enabled</code>
Aliases	<code>org.forgerock.agents.config.change.notifications.enabled</code> Introduced in Java Agent 5.6 <code>com.sun.identity.agents.config.change.notification.enable</code> Introduced in Java Agent 5.0 <u>Recognized</u> from AM 6
Type	Boolean: <code>true</code> returns true; all other strings return <code>false</code> .
Default	<code>true</code>
Bootstrap property	Yes
Required property	No
Restart required	No
Local configuration file	<code>AgentBootstrap.properties</code>
AM console	Tab: Global Title: Enable Notifications of Agent Configuration Change Legacy title: Agent Configuration Change Notification

Obsolete Notification URL (deprecated)

Nominates a URI representing a dummy endpoint within the agent, which accepts incoming notifications from AM.

This mechanism was replaced by websocket notifications, so if anything is sent to this dummy endpoint, it will not be processed, but will be acknowledged with "OK".

Property name	<code>org.forgerock.agents.obsolete.notification.url</code>
Deprecated in	5.6
Aliases	<code>com.sun.identity.client.notification.url</code> Introduced in Java Agent 5.0 <u>Recognized</u> from AM 6 <code>org.forgerock.agents.obsolete.notification.url</code> Introduced in Java Agent 5.6
Type	String
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>

Enable Notification of Session Logout (deprecated)

Use [Enable Notification of Session Logout](#) instead of this property.

Flag to indicate whether the agent polls AM for session status updates.

Default: `false`

Property name	<code>com.ipplanet.am.session.client.polling.enabled</code>
Deprecated in	5.6
Aliases	<code>com.ipplanet.am.session.client.polling.enabled</code> Introduced in Java Agent 5.6 <code>com.ipplanet.am.session.client.polling.enable</code> Introduced in Java Agent 5.0 <u>Recognized</u> from AM 6

Type	Boolean: true returns true; all other strings return false .
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	AgentConfig.properties

Enable Notification of Policy Changes

Flag to indicate whether the agent subscribes to WebSocket notifications from AM for policy changes.

Property name	org.forgerock.agents.policy.change.notifications.enabled
Aliases	org.forgerock.agents.policy.change.notifications.enabled Introduced in Java Agent 5.6 com.sun.identity.agents.notification.enabled Introduced in Java Agent 5.0 <u>Recognized</u> from AM 6
Type	Boolean: true returns true; all other strings return false .
Default	true
Bootstrap property	Yes
Required property	No
Restart required	No
Local configuration file	AgentBootstrap.properties
AM console	Tab: AM Services Title: Enable Notification of Policy Changes

Enable Notification of Session Logout

Flag to indicate whether the agent subscribes to WebSocket notifications from AM for session logout.

Default: true

Property name	org.forgerock.agents.session.change.notification.s.enabled
Aliases	org.forgerock.agents.session.change.notification.s.enabled Introduced in Java Agent 5.6 <u>Recognized</u> from AM 7
Type	Boolean: true returns true; all other strings return false.
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	AgentConfig.properties
AM console	Tab: Global (from AM 7) Title: Enable Notification of Session Logout

POST data preservation

POST Data Preservation Directory Sweep Interval

The interval in seconds at which the POST Data Preservation File Directory is swept for expired files. Files expire after the time defined by POST Data Preservation Cache TTL.

This property is valid only when Enable POST Data Preservation and POST Data Preservation in Files or Cache are true, and POST Data Preservation File Directory is a valid directory.

Property name	org.forgerock.agents.pdp.directory.sweep.seconds
---------------	--

Aliases	<code>org.forgerock.agents.pdp.directory.sweep.seconds</code> Introduced in Java Agent 5.10.0
Type	Integer
Default	10
Bootstrap property	Yes
Required property	No
Restart required	Yes - Restart the container after changing the property
Local configuration file	<code>AgentBootstrap.properties</code>

Missing POST Data Preservation Entry URI Map

A map of URLs to which the agent redirects when the POST data preservation cache entry is discarded due to a cache timeout. The URL is expected to be a page explaining what has happened.

Property name	<code>org.forgerock.agents.pdp.noentry.url.map</code>
Aliases	<code>org.forgerock.agents.pdp.noentry.url.map</code> Introduced in Java Agent 5.6 <code>com.sun.identity.agents.config.postdata.preserve.cache.noentry.url</code> Introduced in Java Agent 5.0 <u>Recognized</u> from AM 6
Type	Map <ul style="list-style-type: none"> • Keys: web application • Values: URL of page explaining the PDP entry was discarded
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>

AM console	Tab: Advanced Title: Missing POST Data Preservation Entry URI Map Legacy title: Missing PDP entry URI
------------	---

POST Data Preservation Cache TTL

The interval in minutes at which entries in the POST data preservation cache timeout and are purged.

If this property and [POST Data Preservation Cache TTL in Milliseconds \(deprecated\)](#) are set, [POST Data Preservation Cache TTL in Milliseconds \(deprecated\)](#) takes precedence.

Property name	<code>org.forgerock.agents.pdp.cache.ttl.minutes</code>
Aliases	<code>org.forgerock.agents.pdp.cache.ttl.minutes</code> Introduced in Java Agent 5.6 <u>Recognized</u> from AM 7
Type	Integer
Default	5
Bootstrap property	Yes
Required property	No
Restart required	Yes - Restart the container after changing the property
Local configuration file	<code>AgentBootstrap.properties</code>
AM console	Tab: Advanced (from AM 7) Title: POST Data Preservation Cache TTL Legacy title: PDP Cache TTL in Minutes

POST Data Preservation Sticky Session Key Value

A name/value pair separated by `=`, as follows:

When [POST Data Preservation Sticky Session Mode](#) is `URL`, this property sets the query parameter name and value.

When POST Data Preservation Sticky Session Mode is `Cookie`, this property sets the cookie name and value.

Property name	<code>org.forgerock.agents.pdp.sticky.session.value</code>
Aliases	<code>com.sun.identity.agents.config.postdata.preserve.stickysession.value</code> Introduced in Java Agent 5.0 <u>Recognized</u> from AM 6 <code>org.forgerock.agents.pdp.sticky.session.value</code> Introduced in Java Agent 5.6
Type	String
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>
AM console	Tab: Advanced Title: POST Data Preservation Sticky Session Key Value Legacy title: PDP Stickysession key-value

POST Data Preservation Sticky Session Mode

Property name	<code>org.forgerock.agents.pdp.sticky.session.mode</code>
Aliases	<code>org.forgerock.agents.pdp.sticky.session.mode</code> Introduced in Java Agent 5.6 <code>com.sun.identity.agents.config.postdata.preserve.stickysession.mode</code> Introduced in Java Agent 5.0 <u>Recognized</u> from AM 6

Supported settings	<p>COOKIE</p> <p>The sticky session mode is sent as a cookie (name/value specified by "POST Data Preservation Sticky Session Key Value" (org.forgerock.agents.pdp.sticky.session.value)).</p> <p>URL</p> <p>The sticky session mode is sent as an HTTP parameter name/value pair (specified by "POST Data Preservation Sticky Session Key Value" (org.forgerock.agents.pdp.sticky.session.value)).</p>
Default	URL
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	AgentConfig.properties
AM console	<p>Tab: Advanced</p> <p>Title: POST Data Preservation Sticky Session Mode</p> <p>Legacy title: PDP Stickysession mode</p>

Enable POST Data Preservation

When `true`, unauthenticated POST data is stored before redirecting to the login screen, then auto-submitted after successful authentication.

Property name	<code>org.forgerock.agents.post.data.preservation.enabled</code>
Aliases	<p><code>org.forgerock.agents.post.data.preservation.enabled</code></p> <p>Introduced in Java Agent 5.6</p> <p><code>com.sun.identity.agents.config.postdata.preserve.enable</code></p> <p>Introduced in Java Agent 5.0</p> <p><u>Recognized</u> from AM 6</p>

Type	Boolean: true returns true; all other strings return false .
Default	false
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	AgentConfig.properties
AM console	Tab: Advanced Title: Enable POST Data Preservation Legacy title: Post Data Preservation enabled

POST Data Preservation in Files or Cache

When [Enable POST Data Preservation](#) is true , this property determines how POST data is saved:

true : Save POST data to files

false (default): Save POST data to the in-memory cache

Files are stored in the [POST Data Preservation File Directory](#). Expired files are removed at the interval given by [POST Data Preservation Directory Sweep Interval](#).

Property name	org.forgerock.agents.pdp.use.filesystem.enabled
Aliases	org.forgerock.agents.pdp.use.filesystem.enabled Introduced in Java Agent 5.10.0
Type	Boolean: true returns true; all other strings return false .
Default	false
Bootstrap property	No
Required property	No
Restart required	No

Local configuration file	AgentConfig.properties
--------------------------	------------------------

Pre-Authn and Post Data Preservation Cookie Signing Value

The key to sign pre-authentication cookies and POST data preservation cookies.

The key is set during installation, when the agent requests the path to a file containing the cookie signing key, and then uses the key to set the cookie signing value in the `AgentKey.properties` file. For information about how to set or change the key after installation, see [Rotate cookie signing keys](#).

For security, you are recommended to configure cookie signing. The agent does not sign cookies when:

- The path to the signing key is left blank during installation.
- The signing key in the `AgentKey.properties` file is less than 64-characters long.

Property name	<code>org.forgerock.agents.cookie.signing.value</code>
Aliases	<code>org.forgerock.agents.cookie.signing.value</code> Introduced in Java Agent 5.10.0
Type	String
Bootstrap property	No
Required property	No
Restart required	Yes - Restart the container after changing the property
Local configuration file	<code>AgentKey.properties</code>

POST Data Preservation Storage Size

The maximum number of megabytes allocated to store POST data. When the maximum is reached, old entries are discarded.

Use this property to mitigate the risk of DDoS attacks.

This property takes precedence over [Max Entries in POST Data Preservation Storage](#).

Property name	<code>org.forgerock.agents.pdp.cache.total.size.mb</code>
---------------	---

Aliases	<p><code>org.forgerock.agents.pdp.cache.total.size.mb</code> Introduced in Java Agent 5.6</p> <p><code>org.forgerock.openam.agents.config.postdata.preserve.cache.entry.max.total.size.mb</code> Introduced in Java Agent 5.6 <u>Recognized</u> from AM 6</p>
Type	Integer
Default	''
Bootstrap property	Yes
Required property	No
Restart required	Yes - Restart the container after changing the property
Local configuration file	AgentBootstrap.properties
AM console	<p>Tab: Advanced</p> <p>Title: POST Data Preservation Storage Size</p> <p>Legacy title: PDP Maximum Cache Size</p>

Max Entries in POST Data Preservation Storage

When POST Data Preservation in Files or Cache is `false`, the maximum number of entries in the POST data preservation storage cache.

When POST Data Preservation in Files or Cache is `true`, the maximum number of files in the POST Data Preservation File Directory.

When the maximum is reached, old entries are discarded.

Use this property to mitigate the risk of DoS attacks.

POST Data Preservation Storage Size takes precedence over this property.

Property name	<code>org.forgerock.agents.pdp.cache.size</code>
---------------	--

Aliases	<p><code>org.forgerock.agents.pdp.cache.size</code> Introduced in Java Agent 5.6</p> <p><code>org.forgerock.openam.agents.config.postdata.preserve.cache.entry.max.entries</code> Introduced in Java Agent 5.6 <u>Recognized</u> from AM 6</p>
Type	Integer
Default	1000
Bootstrap property	Yes
Required property	No
Restart required	Yes - Restart the container after changing the property
Local configuration file	AgentBootstrap.properties
AM console	<p>Tab: Advanced</p> <p>Title: Max Entries in POST Data Preservation Storage</p> <p>Legacy title: PDP Maximum Number of Cache Entries</p>

POST Data Preservation File Directory

When [Enable POST Data Preservation](#) and [POST Data Preservation in Files or Cache](#) are true, this property defines the directory in which POST data preservation data files are saved.

The agent must be able to access the directory. If the directory does not exist, or the agent cannot access it, [Enable POST Data Preservation](#) is set to false.

Default: `/path/to/java_agents/agent_type/Agent_n/pdp`.

Property name	<code>org.forgerock.agents.pdp.directory</code>
Aliases	<p><code>org.forgerock.agents.pdp.directory</code> Introduced in Java Agent 5.10.0</p>
Type	String
Bootstrap property	No

Required property	No
Restart required	No
Local configuration file	AgentConfig.properties

Post Data Preservation Cookie Name

The name of the Post Data Preservation cookie. This cookie maintains the security of the data in unauthenticated POST requests. It contains a unique one-time code which is cross-checked against the stored data making it extremely difficult for malicious actors to replay the stored data for other users.

Since Java Agent 5.10, there is the option of creating one cookie for all concurrent PDP requests, or alternatively to have one uniquely named cookie per request.

If you have tests in your environment that make multiple PDP requests to the agent, you may find intermittent failures as browsers can limit how many cookies they handle.

Configure the cookie name as follows:

- To use one cookie for all concurrent PDP requests to AM, configure as a string. For example, `org.forgerock.agents.pdp.cookie.name=cookie-name`.
- To use one cookie for each authentication request to AM, configure as `%n` before, in the middle, or after a string. When the agent creates the cookie, it substitutes `%n` for a unique identifier. For example:
 - `org.forgerock.agents.pdp.cookie.name=%n`
 - `org.forgerock.agents.pdp.cookie.name=%n-cookie-name`
 - `org.forgerock.agents.pdp.cookie.name=cookie-%n-name`
 - `org.forgerock.agents.pdp.cookie.name=cookie-name-%n`

The agent compresses and then signs the cookie.

Property name	<code>org.forgerock.agents.pdp.cookie.name</code>
Aliases	<code>org.forgerock.agents.pdp.cookie.name</code> Introduced in Java Agent 5.10.0 <u>Recognized</u> from AM 7.1
Type	String
Default	PDP_Nonce

Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	AgentConfig.properties

POST Data Preservation Cache TTL in Milliseconds (deprecated)

Specifies the POST data preservation cache timeout in milliseconds.

Use [POST Data Preservation Cache TTL](#) instead of this property.

If this property and [POST Data Preservation Cache TTL](#) are set, this property takes precedence.

Property name	com.sun.identity.agents.config.postdata.preserve.cache.entry.ttl
Deprecated in	5.6
Aliases	com.sun.identity.agents.config.postdata.preserve.cache.entry.ttl Introduced in Java Agent 5.0
Type	Integer
Default	-2147483648
Bootstrap property	Yes
Required property	No
Restart required	Yes - Restart the container after changing the property
Local configuration file	AgentBootstrap.properties

Policy enforcement

POST Parameter List for URL Policy Env

The list of HTTP POST request parameters whose names and values the agent sets in the environment map for URL policy evaluation by the AM server.

Property name	<code>org.forgerock.agents.continuous.security.post.list</code>
Aliases	<code>com.sun.identity.agents.config.policy.env.post.param</code> Introduced in Java Agent 5.0 <u>Recognized</u> from AM 6 <code>org.forgerock.agents.continuous.security.post.list</code> Introduced in Java Agent 5.7
Type	List
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>
AM console	Tab: AM Services Title: POST Parameter List for URL Policy Env Legacy title: URL Policy Env POST Parameters

Max Entries in Policy Cache per Session

The maximum number of policy evaluation entries allowed in the policy evaluation cache for each session.

The number of policy evaluation results that can be stored is this property multiplied by the value of Max Sessions in Policy Cache.

Property name	<code>org.forgerock.agents.policy.cache.per.session.size</code>
---------------	---

Aliases	<p><code>com.sun.identity.policy.client.cacheResultsPerUserCap</code> Introduced in Java Agent 5.0</p> <p><code>org.forgerock.agents.policy.cache.per.session.size</code> Introduced in Java Agent 5.6 <u>Recognized</u> from AM 7</p>
Type	Integer
Default	50
Bootstrap property	Yes
Required property	No
Restart required	Yes - Restart the container after changing the property
Local configuration file	<code>AgentBootstrap.properties</code>
AM console	<p>Tab: Advanced (from AM 7)</p> <p>Title: Max Entries in Policy Cache per Session</p> <p>Legacy title: Policy Cache Per User</p>

Restrict to Realm Map

A map to restrict access to the specified web application to users authenticated in the specified realm.

Property name	<code>org.forgerock.agents.restrict.to.realm.map</code>
Aliases	<p><code>org.forgerock.agents.restrict.to.realm.map</code> Introduced in Java Agent 5.6.2.1 <u>Recognized</u> from AM 7</p>
Type	<p>Map</p> <ul style="list-style-type: none"> • Keys: web application • Values: allowed realms as CSV
Bootstrap property	No

Required property	No
Restart required	No
Local configuration file	AgentConfig.properties
AM console	Tab: AM Services (from AM 7) Title: Restrict to Realm Map Legacy title: Restrict To Realm

Enable Composite Advice Encoding

When `true`, composite advices are base64 URL-encoded before being sent to custom login endpoints. Use this property to increase security, and protect against cross-site scripting attacks.

Property name	<code>org.forgerock.agents.advice.b64.url.encode.enabled</code>
Aliases	<code>com.forgerock.agents.advice.b64.url.encode</code> Introduced in Java Agent 5.6.2.1 <u>Recognized</u> from AM 7 <code>org.forgerock.agents.advice.b64.url.encode.enabled</code> Introduced in Java Agent 5.6.2.1 <code>org.forgerock.agents.advice.b64.url.encode</code> Introduced in Java Agent 5.6.2.1
Type	Boolean: <code>true</code> returns true; all other strings return <code>false</code> .
Default	<code>false</code>
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	AgentConfig.properties

AM console	Tab: AM Services (from AM 7) Title: Enable Composite Advice Encoding Legacy title: Composite Advice Encode
------------	--

Max Sessions in Policy Cache

The maximum number of sessions (distinct users) that can be stored in the policy evaluation cache at any time.

Property name	<code>org.forgerock.agents.policy.cache.session.size</code>
Aliases	<code>org.forgerock.agents.policy.cache.session.size</code> Introduced in Java Agent 5.6 <u>Recognized</u> from AM 7 <code>com.sun.identity.policy.client.cachedSessionCap</code> Introduced in Java Agent 5.0
Type	Integer
Default	5000
Bootstrap property	Yes
Required property	No
Restart required	Yes - Restart the container after changing the property
Local configuration file	<code>AgentBootstrap.properties</code>
AM console	Tab: Advanced (from AM 7) Title: Max Sessions in Policy Cache Legacy title: Policy Cache Size

Enable Policy Evaluation in User Authentication Realm

When `true`, perform policy evaluation in the realm to which the user is authenticated, and ignore the value in [Policy Evaluation Realm Map](#).

Use this property for web applications that dynamically set the realm for authentication.

Property name	<code>org.forgerock.agents.user.realm.overrides.policy.evaluation.realm.enabled</code>
Aliases	<code>org.forgerock.agents.user.realm.overrides.policy.evaluation.realm.enabled</code> Introduced in Java Agent 5.7.1 <u>Recognized</u> from AM 7.1
Type	Boolean: true returns true; all other strings return false.
Default	false
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>
AM console	Tab: AM Services (from AM 7.1) Title: Enable Policy Evaluation in User Authentication Realm Legacy title: Perform Policy Evaluation in User Authenticated Realm

GET Parameter List for URL Policy Env

The list of HTTP GET request parameters whose names and values the agent sets in the environment map for URL policy evaluation by the AM server.

Property name	<code>org.forgerock.agents.continuous.security.get.list</code>
Aliases	<code>com.sun.identity.agents.config.policy.env.get.param</code> Introduced in Java Agent 5.0 <u>Recognized</u> from AM 6 <code>org.forgerock.agents.continuous.security.get.list</code> Introduced in Java Agent 5.7

Type	List
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	AgentConfig.properties
AM console	Tab: AM Services Title: GET Parameter List for URL Policy Env Legacy title: URL Policy Env GET Parameters

Policy Cache TTL

The interval in minutes at which entries in the policy cache time out and are purged.

Property name	org.forgerock.agents.policy.cache.ttl.minutes
Aliases	org.forgerock.agents.policy.cache.ttl.minutes Introduced in Java Agent 5.6 com.sun.identity.agents.polling.interval Introduced in Java Agent 5.0 <u>Recognized</u> from AM 7
Type	Integer
Default	3
Bootstrap property	Yes
Required property	No
Restart required	Yes - Restart the container after changing the property
Local configuration file	AgentBootstrap.properties
AM console	Tab: Advanced Title: Policy Cache TTL

JSession Parameter List for URL Policy Env

The list of HTTP session attributes whose names and values the agent sets in the environment map for URL policy evaluation by the AM server.

Property name	<code>org.forgerock.agents.continuous.security.http.session.list</code>
Aliases	<code>org.forgerock.agents.continuous.security.http.session.list</code> Introduced in Java Agent 5.7 <code>com.sun.identity.agents.config.policy.env.jsession.param</code> Introduced in Java Agent 5.0 <u>Recognized</u> from AM 6
Type	List
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>
AM console	Tab: AM Services Title: JSession Parameter List for URL Policy Env Legacy title: URL Policy Env jsession Parameters

Policy Evaluation Realm Map

The name of an AM realm to use for policy evaluations. Different web applications can use different policy realms.

NOTE

To prevent errors, use only characters in the standard ASCII set. The agent automatically percent-encodes characters in the extended ASCII set, however, the name must be manually encoded in AM.

Property name	<code>org.forgerock.agents.policy.evaluation.realm.map</code>
---------------	---

Aliases	<p><code>org.forgerock.openam.agents.config.policy.evaluation.realm</code></p> <p>Introduced in Java Agent 5.0 <u>Recognized</u> from AM 6</p> <p><code>org.forgerock.agents.policy.evaluation.realm.map</code></p> <p>Introduced in Java Agent 5.6.2.1</p>
Type	<p>Map</p> <ul style="list-style-type: none"> • Keys: web application • Values: realm
Default	/
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>
AM console	<p>Tab: AM Services</p> <p>Title: Policy Evaluation Realm Map</p> <p>Legacy title: Policy Evaluation Realm</p>

Policy Set Map

The name of an AM policy set to use for policy evaluations. Different web applications can use a different policy set in their chosen realm.

NOTE

To prevent errors, use only characters in the standard ASCII set. The agent automatically percent-encodes characters in the extended ASCII set, however, the name must be manually encoded in AM.

The following example causes AM to use `mypolicyset` to evaluate policies for all web applications:

```
org.forgerock.agents.policy.set.map=mypolicyset
```

The following example causes AM to use `mypolicyset` to evaluate policies for `mywebapp`. For all other web applications, AM uses `iPlanetAMWebAgentService`:

`org.forgerock.agents.policy.set.map[mywebapp]=mypolicyset`

Property name	<code>org.forgerock.agents.policy.set.map</code>
Aliases	<code>org.forgerock.openam.agents.config.policy.evaluation.application</code> Introduced in Java Agent 5.0 <u>Recognized</u> from AM 6 <code>org.forgerock.agents.policy.set.map</code> Introduced in Java Agent 5.6.2.1
Type	Map <ul style="list-style-type: none">• Keys: web application• Values: policy set
Default	<code>iPlanetAMWebAgentService</code>
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>
AM console	Tab: AM Services Title: Policy Set Map Legacy title: Policy Set

Port check

Port Check Filename (deprecated)

Nominates a file containing port numbers to be checked when port checking is enabled. See [Enable Port Checking \(deprecated\)](#).

Property name	<code>org.forgerock.agents.port.check.file</code>
Deprecated in	5.6

Aliases	<p><code>com.sun.identity.agents.config.port.check.file</code> Introduced in Java Agent 5.0 <u>Recognized</u> from AM 6</p> <p><code>org.forgerock.agents.port.check.file</code> Introduced in Java Agent 5.6</p>
Type	String
Default	<code>PortCheckContent.txt</code>
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>
AM console	<p>Tab: Miscellaneous</p> <p>Title: Port Check Filename</p> <p>Legacy title: Port Check File</p>

Port Check Protocol Map (deprecated)

A map of allowed protocols for each port, valid when port checking is enabled. See [Enable Port Checking \(deprecated\)](#).

Property name	<code>org.forgerock.agents.port.check.map</code>
Deprecated in	5.6
Aliases	<p><code>com.sun.identity.agents.config.port.check.setting</code> Introduced in Java Agent 5.0 <u>Recognized</u> from AM 6</p> <p><code>org.forgerock.agents.port.check.map</code> Introduced in Java Agent 5.6</p>
Type	<p>Map</p> <ul style="list-style-type: none"> • Keys: port number • Values: protocol scheme

Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	AgentConfig.properties
AM console	Tab: Miscellaneous Title: Port Check Protocol Map Legacy title: Port Check Setting

Enable Port Checking (deprecated)

A flag to enable port checking when the filter mode is `SSO_ONLY`. See [Agent Filter Mode Map](#).

Property name	<code>org.forgerock.agents.port.check.enabled</code>
Deprecated in	5.6
Aliases	<code>com.sun.identity.agents.config.port.check.enable</code> Introduced in Java Agent 5.0 <u>Recognized</u> from AM 6 <code>org.forgerock.agents.port.check.enabled</code> Introduced in Java Agent 5.6
Type	Boolean: <code>true</code> returns true; all other strings return <code>false</code> .
Default	<code>false</code>
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	AgentConfig.properties

AM console	Tab: Miscellaneous Title: Enable Port Checking Legacy title: Port Check Enable
------------	--

Pre-authentication

Pre-Authn and Post Data Preservation Cookie Signing Value

The key to sign pre-authentication cookies and POST data preservation cookies.

The key is set during installation, when the agent requests the path to a file containing the cookie signing key, and then uses the key to set the cookie signing value in the `AgentKey.properties` file. For information about how to set or change the key after installation, see [Rotate cookie signing keys](#).

For security, you are recommended to configure cookie signing. The agent does not sign cookies when:

- The path to the signing key is left blank during installation.
- The signing key in the `AgentKey.properties` file is less than 64-characters long.

Property name	<code>org.forgerock.agents.cookie.signing.value</code>
Aliases	<code>org.forgerock.agents.cookie.signing.value</code> Introduced in Java Agent 5.10.0
Type	String
Bootstrap property	No
Required property	No
Restart required	Yes - Restart the container after changing the property
Local configuration file	<code>AgentKey.properties</code>

Max Age of Pre-Authentication Cookie

The maximum age in seconds of the pre-authentication cookie configured in [Pre-Authentication Cookie Name](#).

Property name	<code>org.forgerock.agents.authn.cookie.max.age.seconds</code>
Aliases	<code>org.forgerock.agents.authn.cookie.max.age.seconds</code> Introduced in Java Agent 5.6.3.0 <u>Recognized</u> from AM 7
Type	Integer
Default	600
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>
AM console	Tab: Global (from AM 7) Title: Max Age of Pre-Authentication Cookie Legacy title: Pre-Authenticated Cookie Max Age

Pre-Authentication Cookie Name

The name of the pre-authentication cookie. This cookie tracks the progress of authentication with AM, and protects requests from replay attacks. It contains the following information:

- URL of the original request
- HTTP mode
- Secure ID (subsequently baked into the nonce of the returned JWT)
- Relevant ACR information
- Transaction ID
- Expiry time configured by Max Age of Pre-Authentication Cookie

(Before Java Agent 5.7), The agent creates a single cookie containing records to identify all concurrent authentication requests to AM. In environments with lots of concurrent requests, or where the protected URLs are long, the cookie can reach the maximum size supported by the browser. When this happens, new authentication requests fail and the agent issues a 403 HTTP message to the user.

(Java Agent 5.7 and later versions) The agent can optionally create a cookie for each authentication request to AM. In some environments, this creates a large number of cookies. If you have tests in your environment that make multiple requests to AM from the same browser, you may find intermittent 403 HTTP messages; browsers can limit how many cookies they handle.

Configure the cookie name as follows:

- To use one cookie for all concurrent authentication requests to AM, configure as a string. For example, `org.forgerock.agents.authn.cookie.name=cookie-name`.
- To use one cookie for each authentication request to AM, configure as `%n`, or as `%n` before, in the middle of, or after a string. When the agent creates the cookie, it translates the string `%n` into a unique identifier. For example:
 - `org.forgerock.agents.authn.cookie.name=%n`
 - `org.forgerock.agents.authn.cookie.name=%n-cookie-name`
 - `org.forgerock.agents.authn.cookie.name=cookie-%n-name`
 - `org.forgerock.agents.authn.cookie.name=cookie-name-%n`

The agent compresses and then signs the cookie.

Property name	<code>org.forgerock.agents.authn.cookie.name</code>
Aliases	<code>com.sun.identity.agents.config.cdsso.cookie.name</code> Introduced in Java Agent 5.0 <u>Recognized</u> from AM 7 <code>org.forgerock.agents.authn.cookie.name</code> Introduced in Java Agent 5.6
Type	String
Default	<code>amFilterCDSSORequest</code>
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>
AM console	Tab: Global (from AM 7) Title: Pre-Authentication Cookie Name Legacy title: Pre-Authenticated Cookie Name

Profile

Fall-Forward Mode (deprecated)

Use [Strategy when AM unavailable](#) instead of this property.

Property name	<code>org.forgerock.agents.fallforward.mode.enabled</code>
Deprecated in	5.9
Aliases	<code>org.forgerock.agents.fallforward.mode.enabled</code> Introduced in Java Agent 5.7 Recognized from AM 7.1
Type	Boolean: true returns true; all other strings return false.
Default	false
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>
AM console	Tab: Global (not available from AM 7.2) Title: Fall-Forward Mode

Location of Agent Configuration Repository

The location of the agent configuration.

Property name	<code>org.forgerock.agents.config.location</code>
---------------	---

Aliases	<code>com.sun.identity.agents.config.repository.location</code> Introduced in Java Agent 5.0 <u>Recognized</u> from AM 6 <code>org.forgerock.agents.config.location</code> Introduced in Java Agent 5.6
Supported settings	LOCAL The agent configuration is read from <code>AgentConfiguration.properties</code> (only). REMOTE The agent configuration is downloaded from AM.
Default	REMOTE
Bootstrap property	Yes
Required property	Yes - If this property is missing, the agent fails to start
Restart required	Yes - Restart the container after changing the property
Local configuration file	<code>AgentBootstrap.properties</code>
AM console	Tab: Global Title: Location of Agent Configuration Repository

JWT Cookie Domain List

A list of domains in which the agent attempts to creates JWT cookies:

- If the list is empty, the agent creates cookies only in its own domain.
- If the agent is running behind a browser, it can create cookies only in its own domain.
- If the agent is running behind a proxy, it should be able to create cookies in any required domains.

Default: Empty

Property name	<code>org.forgerock.agents.jwt.cookie.domain.list</code>
---------------	--

Aliases	<p><code>com.sun.identity.agents.config.cdsso.domain</code> Introduced in Java Agent 5.0 <u>Recognized</u> from AM 6</p> <p><code>org.forgerock.agents.jwt.cookie.domain.list</code> Introduced in Java Agent 5.6</p>
Type	List
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>
AM console	<p>Tab: SSO (from AM 7.1)</p> <p>Title: JWT Cookie Domain List</p> <p>Legacy title: CDSSO Domain List</p>

JWT Cache TTL

The interval in minutes at which entries in the JWT cache timeout and are purged.

Parsing JWTs is a CPU intensive process. As all JWTs in the cache have already been parsed, consider using a long timeout for this cache.

Property name	<code>org.forgerock.agents.jwt.cache.ttl.minutes</code>
Aliases	<p><code>org.forgerock.openam.agents.config.jwt.cache.ttl.minutes</code> Introduced in Java Agent 5.0 <u>Recognized</u> from AM 7</p> <p><code>org.forgerock.agents.jwt.cache.ttl.minutes</code> Introduced in Java Agent 5.6</p>
Type	Integer
Default	30
Bootstrap property	Yes

Required property	No
Restart required	Yes - Restart the container after changing the property
Local configuration file	AgentBootstrap.properties
AM console	Tab: Advanced (from AM 7) Title: JWT Cache TTL

Max Entries in JWT Cache

The maximum number of entries in the JWT cache.

Property name	<code>org.forgerock.agents.jwt.cache.size</code>
Aliases	<code>org.forgerock.agents.jwt.cache.size</code> Introduced in Java Agent 5.6 <code>org.forgerock.openam.agents.config.jwt.cache.size</code> Introduced in Java Agent 5.0 <u>Recognized</u> from AM 7
Type	Integer
Default	5000
Bootstrap property	Yes
Required property	No
Restart required	Yes - Restart the container after changing the property
Local configuration file	AgentBootstrap.properties
AM console	Tab: Advanced (from AM 7) Title: Max Entries in JWT Cache Legacy title: JWT Cache Size

JWT Cookie Name

The name of the cookie that holds the OIDC JWT on the user's browser.

Before changing the name of this cookie, consider the following points:

- This cookie is only used by the agent and is never presented to AM.
- The cookie name must be unique in the cookies the user's browser receives. For example, do not set the JWT cookie name to `iPlanetDirectoryPro`, which is the default name of the AM session cookie.

If the agent does not find the cookie named by JWT Cookie Name, authentication fails. The user can only access resources that are available through not-enforced rules.

Property name	<code>org.forgerock.agents.jwt.cookie.name</code>
Aliases	<code>org.forgerock.openam.agents.config.jwt.name</code> Introduced in Java Agent 5.0 <u>Recognized</u> from AM 6 <code>org.forgerock.agents.jwt.cookie.name</code> Introduced in Java Agent 5.6
Type	String
Default	<code>am-auth-jwt</code>
Bootstrap property	Yes
Required property	No
Restart required	No
Local configuration file	<code>AgentBootstrap.properties</code>
AM console	Tab: Global Title: JWT Cookie Name

Agent Profile Realm

The realm in which the agent profile is defined.

When Enable Policy Evaluation in User Authentication Realm is `true`, AM uses this realm to evaluate policies for policy decision requests from the agent.

Property name	<code>org.forgerock.agents.agent.profile.realm</code>
---------------	---

Aliases	org.forgerock.agents.agent.profile.realm Introduced in Java Agent 5.6 com.sun.identity.agents.config.organization.name Introduced in Java Agent 5.0
Type	String
Default	/
Bootstrap property	Yes
Required property	Yes - If this property is missing, the agent fails to start
Restart required	Yes - Restart the container after changing the property
Local configuration file	AgentBootstrap.properties

Exchanged SSO Token Cache TTL

The interval in minutes at which entries in the SSO token exchange cache timeout and are purged.

The exchanged JWT is cached against the relevant SSO token. If the same SSO token is presented again, before the cache entry expires, the agent does not need to exchange the token again, but retrieves the one stored in its cache.

Because exchanging SSO tokens for JWTs is an expensive process, previously exchanged SSO tokens are cached. When an entity is unable to permanently store its JWT in a cookie, calls to AM can be avoided.

Property name	org.forgerock.agents.sso.exchange.cache.ttl.minutes
Aliases	org.forgerock.agents.sso.exchange.cache.ttl.minutes Introduced in Java Agent 5.6.2.1 <u>Recognized</u> from AM 7
Type	Integer
Default	5
Bootstrap property	Yes
Required property	No

Restart required	Yes - Restart the container after changing the property
Local configuration file	AgentBootstrap.properties
AM console	<p>Tab: Advanced (from AM 7)</p> <p>Title: Exchanged SSO Token Cache TTL</p> <p>Legacy title: Exchanged SSO Token Cache Time to Live</p>

Configuration Reload Interval

When the Location of Agent Configuration Repository is LOCAL , this is the number of seconds after which the agent reloads its configuration if it has been changed since it was last read.

Property name	org.forgerock.agents.config.reload.seconds
Aliases	<p>com.sun.identity.agents.config.load.interval Introduced in Java Agent 5.0 <u>Recognized</u> from AM 6</p> <p>org.forgerock.agents.config.reload.seconds Introduced in Java Agent 5.6</p>
Type	Integer
Default	0
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	AgentConfig.properties
AM console	<p>Tab: Global</p> <p>Title: Configuration Reload Interval</p>

Agent Profile Name

The profile name used to fetch agent configuration data from AM, to evaluate policies for users, retrieve session info, and so on.

Default: Empty

Property name	<code>org.forgerock.agents.profile.name</code>
Aliases	<code>com.sun.identity.agents.app.username</code> Introduced in Java Agent 5.0 <code>com.sun.identity.agents.config.profilename</code> Introduced in Java Agent 5.0 <code>org.forgerock.agents.profile.name</code> Introduced in Java Agent 5.6
Type	String
Bootstrap property	Yes
Required property	Yes - If this property is missing, the agent fails to start
Restart required	Yes - Restart the container after changing the property
Local configuration file	<code>AgentBootstrap.properties</code>

Enable Configuration Lock

When `true`, an agent restart is required to allow configuration changes, even for hot-swappable parameters.

Property name	<code>org.forgerock.agents.lock.config.enabled</code>
Aliases	<code>com.sun.identity.agents.config.lock.enable</code> Introduced in Java Agent 5.0 <code>org.forgerock.agents.lock.config.enabled</code> Introduced in Java Agent 5.6
Type	Boolean: <code>true</code> returns true; all other strings return <code>false</code> .
Default	<code>false</code>
Bootstrap property	Yes

Required property	No
Restart required	No
Local configuration file	AgentBootstrap.properties

Profile Attribute Map

Map the value of an AM profile attribute to one or more HTTP headers, HTTP cookies, or request attributes, depending on the value of [Profile Attribute Fetch Mode](#).

- Map key: The name of an AM profile attribute
- Map value: The name of one or more HTTP headers, HTTP cookies, or request attributes

The user profile can be stored in LDAP or any other arbitrary data store

Consider the following points for HTTP cookies:

- If an HTTP cookie with the mapped name does not exist, the agent creates it.
- If an HTTP cookie with the mapped name already exists and the cookie value is different from the mapped value, the agent overwrites the cookie.
- If an HTTP cookie with the mapped name already exists and the cookie value is the same as the mapped value, the agent does nothing.
- If the profile attribute name (key) does not exist, the agent does not create the HTTP cookie.
- The agent does not automatically clear cookies. To prevent a build up of cookies, consider adding them to the [Reset Cookie List](#).

Consider the following points for HTTP headers:

- If an HTTP header with the mapped name does not exist, the agent creates it.
- If an HTTP header with the mapped name already exists, the agent does not overwrite it but simply appends information to the header.
- If the profile attribute name (key) does not exist, the agent does not create the HTTP header.
- When an HTTP header name is used in a request header, it is prefixed by HTTP_ . The agent automatically changes lower case letters to upper case, and hyphens (-) to underscores (_). For example, CUSTOM-userid becomes HTTP_CUSTOM_USERID .

Format: profile attribute = HEADER-NAME(S) , profile attribute = COOKIE-NAME(S) , profile attribute = REQUEST-ATTRIBUTE(S)

Default: Empty

Examples:

In the following example, the AM response attribute `uid` is mapped to `CUSTOM-User-Name`: `com.sun.identity.agents.config.response.attribute.mapping[uid]=Custom-User-Name`

Example: `[cn]=HEADER-1|HEADER-2`

Property name	<code>org.forgerock.agents.profile.attribute.map</code>
Aliases	<code>com.sun.identity.agents.config.profile.attribute.mapping</code> Introduced in Java Agent 5.0 <u>Recognized</u> from AM 6 <code>org.forgerock.agents.profile.attribute.map</code> Introduced in Java Agent 5.6
Type	Map <ul style="list-style-type: none">• Keys: source response profile name• Values: one or more target response profile names
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>
AM console	Tab: Application Title: Profile Attribute Map Legacy title: Profile Attribute Mapping

Max Entries in SSO Exchange Cache

The maximum number of entries in the SSO exchange cache, used when SSO tokens are exchanged for JWTs.

When the maximum is reached, the oldest records are overwritten.

Property name	<code>org.forgerock.agents.sso.exchange.cache.size</code>
Aliases	<code>org.forgerock.agents.sso.exchange.cache.size</code> Introduced in Java Agent 5.6.2.1 <u>Recognized</u> from AM 7
Type	Integer
Default	100
Bootstrap property	Yes
Required property	No
Restart required	Yes - Restart the container after changing the property
Local configuration file	<code>AgentBootstrap.properties</code>
AM console	Tab: Advanced (from AM 7) Title: Max Entries in SSO Exchange Cache Legacy title: Exchanged SSO Token Cache Size

Profile Attribute Fetch Mode

Map the name of an AM profile attribute specified in [Profile Attribute Map](#) as follows:

- NONE: Do not map
- HTTP_HEADER: Map the to the name of an HTTP profile header
- HTTP_COOKIE: Map to the name of an HTTP cookie
- REQUEST_ATTRIBUTE: Map to the name of an HTTP profile attribute

Property name	<code>org.forgerock.agents.profile.attribute.fetch.mode</code>
Aliases	<code>com.sun.identity.agents.config.profile.attribute.fetch.mode</code> Introduced in Java Agent 5.0 <u>Recognized</u> from AM 6 <code>org.forgerock.agents.profile.attribute.fetch.mode</code> Introduced in Java Agent 5.6

Supported settings	<p>NONE No AM attributes are mapped.</p> <p>HTTP_HEADER The named AM attributes are mapped to headers in the outgoing HTTP response.</p> <p>REQUEST_ATTRIBUTE The named AM attributes are mapped to request attributes in the outgoing HTTP response.</p> <p>HTTP_COOKIE The named AM attributes are mapped to cookies in the outgoing HTTP response.</p>
Default	NONE
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	AgentConfig.properties
AM console	<p>Tab: Application</p> <p>Title: Profile Attribute Fetch Mode</p>

WebSocket Connection Interval

The interval in minutes at which WebSockets to AM are killed and reopened. This property helps ensure a balanced distribution of connections across the AM servers on the site.

Property name	<code>org.forgerock.agents.balance.websocket.interval.minutes</code>
Aliases	<p><code>org.forgerock.openam.agents.config.balance.websocket.connection.interval.in.minutes</code> Introduced in Java Agent 5.6 <u>Recognized</u> from AM 6</p> <p><code>org.forgerock.agents.balance.websocket.interval.minutes</code> Introduced in Java Agent 5.6</p>

Type	Integer
Default	30
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	AgentConfig.properties
AM console	Tab: Global Title: WebSocket Connection Interval

Query parameter

Regex Remove Query Parameters List for Policy Evaluation

A list of regular expressions the agent uses to match query parameters to be removed from the incoming URL for policy evaluation and caching purposes. The property has the following format, with no spaces between values:

```
[Domain[/path]]|parameter[,parameter...]
```

Consider the following constraints when constructing your list of regular expressions:

- Add a comma (,) character at the beginning or the end of the list to remove all unnamed parameters. For example, `myapp.example.com/customers|,lang` would match both `lang` and any unnamed parameters.
- Consider creating multiple simple regular expressions instead of a single complicated one.
- The remaining parameters (those that do not match the list of parameters) are sorted alphabetically.

Examples:

```
org.forgerock.agents.unwanted.http.url.params.regex.list[0]=myapp.example.com|b.*,gp(a|p|s),
```

```
org.forgerock.agents.unwanted.http.url.params.regex.list[1]=|.*
```

The following incoming URL request that matches a rule such as `myapp.example.com/customers|, coun.*?` :

```
http://myapp.example.com/customers?
country=uk&=bristol&lang=en_GB&area=1343456
```

It is cached by the agent as `http://myapp.example.com/customers?
=bristol&lang=en_GB`, where both `country` and unnamed parameter are removed and the remaining parameters are sorted alphabetically.

Property name	<code>org.forgerock.agents.unwanted.http.url.params.regex.list</code>
Aliases	<code>org.forgerock.agents.unwanted.http.url.params.regex.list</code> Introduced in Java Agent 5.6 <code>org.forgerock.openam.agents.config.conditional.unwanted.http.url.params.regex</code> Introduced in Java Agent 5.6 <u>Recognized</u> from AM 7 <code>org.forgerock.agents.unwanted.http.url.params.regex.list</code> Introduced in Java Agent 5.6
Type	List
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>
AM console	Tab: Miscellaneous (from AM 7) Title: Regex Remove Query Parameters List for Policy Evaluation Legacy title: Regular Expression Remove Query Parameters

Remove Query Parameters List for Policy Evaluation

A list of query parameters to be removed from the incoming URL for policy evaluation and caching.

The property has the following format, with no spaces between values:

```
[Domain[/path]]|parameter[,parameter...]
```

Consider the following constraints when constructing the list of parameters:

- Add a comma (,) character at the beginning or the end of the list to remove all unnamed parameters. The following example would match both lang and any unnamed parameters: `myapp.example.com/customers|,lang`
- Add the asterisk (*) character to the list to remove all parameters, including unnamed ones.
- The remaining parameters (those that do not match the list of parameters) are sorted alphabetically.

Examples:

```
org.forgerock.agents.unwanted.http.url.param.list[0]=myapp.example.com/customers|location,lang
```

```
org.forgerock.agents.unwanted.http.url.param.list[1]=example.com/customers|*
```

The following incoming URL request matches a rule such as

```
myapp.example.com/customers|,lang:
```

```
http://myapp.example.com/customers?country=uk&=bristol&lang=en_GB&area=1343456
```

It is cached by the agent as `http://myapp.example.com/customers?area=1343456&country=uk`, where both lang and the unnamed parameter are removed and the rest of the parameters are sorted alphabetically.

Property name	<code>org.forgerock.agents.unwanted.http.url.param.list</code>
Aliases	<code>org.forgerock.agents.unwanted.http.url.param.list</code> Introduced in Java Agent 5.6 <code>org.forgerock.openam.agents.config.conditional.unwanted.http.url.params</code> Introduced in Java Agent 5.6 Recognized from AM 7
Type	List

Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	AgentConfig.properties
AM console	<p>Tab: Miscellaneous (from AM 7)</p> <p>Title: Remove Query Parameters List for Policy Evaluation</p> <p>Legacy title: Remove Query Parameters</p>

Regex Query Parameters List for Policy Evaluation

A list of regular expressions the agent uses to match query parameters, for policy evaluation and caching.

The property has the following format, with no spaces between values:

[Domain[/path]]|regexp[, regexp, ...]

Property name	org.forgerock.agents.wanted.http.url.params.regexp.list
Aliases	<p>org.forgerock.agents.wanted.http.url.params.regexp.list Introduced in Java Agent 5.6</p> <p>org.forgerock.openam.agents.config.conditional.wanted.http.url.params.regexp Introduced in Java Agent 5.6 <u>Recognized</u> from AM 7</p> <p>org.forgerock.agents.wanted.http.url.params.regex.list Introduced in Java Agent 5.6</p>
Type	List
Bootstrap property	No
Required property	No

Restart required	No
Local configuration file	AgentConfig.properties
AM console	Tab: Miscellaneous (from AM 7) Title: Regex Query Parameters List for Policy Evaluation

Query Parameter List for Policy Evaluation

A list of query parameters to be retained for policy evaluation and caching purposes. The property has the following format, with no spaces between values:

```
[Domain[/path]]|parameter[,parameter...]
```

Consider the following constraints when constructing the list of parameters:

- Add a comma (,) character at the beginning or the end of the list to retain all unnamed parameters. For example, `myapp.example.com/customers|,lang` matches both `lang` and any unnamed parameters.
- Add the asterisk (*) character to the list to retain all parameters, including unnamed ones.
- The remaining parameters (those that match the list of parameters) are sorted alphabetically.

Examples:

```
org.forgerock.agents.wanted.http.url.param.list[0]=myapp.example.com/news|area
```

```
org.forgerock.agents.wanted.http.url.param.list[1]=example.com/news|area,country,location,
```

The following incoming URL request matches a rule such as `myapp.example.com/customers|,lang`:

```
http://myapp.example.com/customers?country=uk&=bristol&lang=en_GB&area=1343456
```

It is cached by the agent as `http://myapp.example.com/customers?=bristol&lang=en_GB`, where both `lang` and the unnamed parameter are retained and sorted alphabetically.

Property name	<code>org.forgerock.agents.wanted.http.url.param.list</code>
---------------	--

Aliases	<p><code>org.forgerock.openam.agents.config.conditional.wanted.http.url.params</code> Introduced in Java Agent 5.6 <u>Recognized</u> from AM 7</p> <p><code>org.forgerock.agents.wanted.http.url.param.list</code> Introduced in Java Agent 5.6</p>
Type	List
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>
AM console	<p>Tab: Miscellaneous (from AM 7)</p> <p>Title: Query Parameter List for Policy Evaluation</p> <p>Legacy title: Retain Query Parameters</p>

Required

AM Authentication Service Path

The path to the AM server.

Property name	<code>org.forgerock.agents.am.path</code>
Aliases	<p><code>com.ipplanet.am.services.deploymentDescriptor</code> Introduced in Java Agent 5.0</p> <p><code>org.forgerock.agents.am.path</code> Introduced in Java Agent 5.6</p>
Type	String
Bootstrap property	Yes
Required property	Yes - If this property is missing, the agent fails to start
Restart required	Yes - Restart the container after changing the property

Local configuration file	AgentBootstrap.properties
--------------------------	---------------------------

Authentication Redirect URI

The URI the agent uses to process authentication requests.

When this property is not defined, the redirect URI is provided by AM.

When this property is defined and Location of Agent Configuration Repository is REMOTE , AM overwrites this property.

If OIDC authentication is being used, changing the value of this property while the agent is running prevents it from functioning. Restart the agent immediately after the value in AM is altered and the properties saved.

Property name	org.forgerock.agents.authn.redirect.uri
Aliases	org.forgerock.agents.authn.redirect.uri Introduced in Java Agent 5.6 com.sun.identity.agents.config.cdssso.redirect.uri Introduced in Java Agent 5.0 <u>Recognized</u> from AM 6
Type	String
Bootstrap property	No
Required property	No
Restart required	Yes - Restart the container after changing the property
Local configuration file	AgentConfig.properties
AM console	Tab: SS0 Title: Authentication Redirect URI Legacy title: CDSSO Redirect URI

Encryption Class

The name of the class to be used by the Java agent to implement encryption and decryption. The class must implement both `com.iplanet.services.util.AMEncryption` and `com.iplanet.services.util.ConfigurableKey`

For details see [Rotate the agent profile password](#)

WARNING

After changing this property, you must re-encrypt the agent profile password.

Property name	<code>org.forgerock.agents.encryptor.classname</code>
Aliases	<code>org.forgerock.agents.encryptor.classname</code> Introduced in Java Agent 5.0 <code>com.iplanet.security.encryptor</code> Introduced in Java Agent 5.0
Type	String
Default	<code>org.forgerock.openam.shared.security.crypto.AESWrapEncryption</code>
Bootstrap property	Yes
Required property	Yes - If this property is missing, the agent fails to start
Restart required	No
Local configuration file	<code>AgentBootstrap.properties</code>

AM Authentication Service Protocol

The protocol used by the AM server. Set to one of the following values:

- HTTP
- HTTPS

Property name	<code>org.forgerock.agents.am.protocol</code>
Aliases	<code>org.forgerock.agents.am.protocol</code> Introduced in Java Agent 5.6 <code>com.iplanet.am.server.protocol</code> Introduced in Java Agent 5.0 Recognized from AM 6

Type	String
Bootstrap property	Yes
Required property	Yes - If this property is missing, the agent fails to start
Restart required	Yes - Restart the container after changing the property
Local configuration file	AgentBootstrap.properties
AM console	Tab: AM Services Title: AM Authentication Service Protocol

Agent Profile Realm

The realm in which the agent profile is defined.

When Enable Policy Evaluation in User Authentication Realm is `true`, AM uses this realm to evaluate policies for policy decision requests from the agent.

Property name	<code>org.forgerock.agents.agent.profile.realm</code>
Aliases	<code>org.forgerock.agents.agent.profile.realm</code> Introduced in Java Agent 5.6 <code>com.sun.identity.agents.config.organization.name</code> Introduced in Java Agent 5.0
Type	String
Default	/
Bootstrap property	Yes
Required property	Yes - If this property is missing, the agent fails to start
Restart required	Yes - Restart the container after changing the property
Local configuration file	AgentBootstrap.properties

Encrypted Agent Password

The agent profile password, which must correspond to the value in AM.

Set this property to the encrypted value of the password, where the password is encrypted using the key in the property [Encryption Key/Salt](#).

Use the following command to get the encrypted value of the password, where `passwordFile` contains only the password followed by a newline, and has the access permission `400`:

```
$ ./agentadmin --encrypt agentInstance passwordFile
```

Default: Empty

Property name	<code>org.forgerock.agents.encrypted.password</code>
Aliases	<code>com.ipplanet.am.service.secret</code> Introduced in Java Agent 5.0 <code>org.forgerock.agents.encrypted.password</code> Introduced in Java Agent 5.6
Type	String
Bootstrap property	No
Required property	Yes - If this property is missing, the agent fails to start
Restart required	Yes - Restart the container after changing the property
Local configuration file	<code>AgentPassword.properties</code>

Location of Agent Configuration Repository

The location of the agent configuration.

Property name	<code>org.forgerock.agents.config.location</code>
Aliases	<code>com.sun.identity.agents.config.repository.location</code> Introduced in Java Agent 5.0 Recognized from AM 6 <code>org.forgerock.agents.config.location</code> Introduced in Java Agent 5.6

Supported settings	<p>LOCAL The agent configuration is read from AgentConfiguration.properties (only).</p> <p>REMOTE The agent configuration is downloaded from AM.</p>
Default	REMOTE
Bootstrap property	Yes
Required property	Yes - If this property is missing, the agent fails to start
Restart required	Yes - Restart the container after changing the property
Local configuration file	AgentBootstrap.properties
AM console	<p>Tab: Global</p> <p>Title: Location of Agent Configuration Repository</p>

Agent Profile Name

The profile name used to fetch agent configuration data from AM, to evaluate policies for users, retrieve session info, and so on.

Default: Empty

Property name	org.forgerock.agents.profile.name
Aliases	<p>com.sun.identity.agents.app.username Introduced in Java Agent 5.0</p> <p>com.sun.identity.agents.config.profilename Introduced in Java Agent 5.0</p> <p>org.forgerock.agents.profile.name Introduced in Java Agent 5.6</p>
Type	String
Bootstrap property	Yes
Required property	Yes - If this property is missing, the agent fails to start
Restart required	Yes - Restart the container after changing the property

Local configuration file	AgentBootstrap.properties
--------------------------	---------------------------

Autonomous mode

When `true` the agent operates independently of AM, without needing to contact an AM instance. Agents allow access to resources as defined in not-enforced lists; otherwise, they deny access.

Property name	<code>org.forgerock.agents.fallback.mode.enabled</code>
Aliases	<code>com.forgerock.agents.config.fallback.mode</code> Introduced in Java Agent 5.9.0 <code>org.forgerock.agents.fallback.mode.enabled</code> Introduced in Java Agent 5.9.0 <code>org.forgerock.agents.autonomous.mode.enabled</code> Introduced in Java Agent 5.9.0
Type	Boolean: <code>true</code> returns true; all other strings return <code>false</code> .
Default	<code>false</code>
Bootstrap property	Yes
Required property	Yes - If this property is missing, the agent fails to start
Restart required	Yes - Restart the container after changing the property
Local configuration file	AgentBootstrap.properties

AM Authentication Service Host Name

The AM server host name.

Property name	<code>org.forgerock.agents.am.hostname</code>
---------------	---

Aliases	<p>com.ip1anet.am.server.host Introduced in Java Agent 5.0 <u>Recognized</u> from AM 6</p> <p>org.forgerock.agents.am.hostname Introduced in Java Agent 5.6</p>
Type	String
Bootstrap property	Yes
Required property	Yes - If this property is missing, the agent fails to start
Restart required	Yes - Restart the container after changing the property
Local configuration file	AgentBootstrap.properties
AM console	<p>Tab: AM Services</p> <p>Title: AM Authentication Service Host Name</p>

AM Authentication Service Port

The AM server port number.

Property name	org.forgerock.agents.am.port
Aliases	<p>com.ip1anet.am.server.port Introduced in Java Agent 5.0 <u>Recognized</u> from AM 6</p> <p>org.forgerock.agents.am.port Introduced in Java Agent 5.6</p>
Type	String
Bootstrap property	Yes
Required property	Yes - If this property is missing, the agent fails to start
Restart required	Yes - Restart the container after changing the property
Local configuration file	AgentBootstrap.properties
AM console	<p>Tab: AM Services</p> <p>Title: AM Authentication Service Port</p>

Public AM URL

The assembled "public" URL of AM. This URL is used by the agent to redirect the user's browser to AM for login (customised or not), or if necessary, exchange an SSO token for a JWT.

The following properties make up the URL:

- [AM Authentication Service Protocol](#)
- [AM Authentication Service Host Name](#)
- [AM Authentication Service Port](#)
- [AM Authentication Service Path](#)

The "private" URL is used by the agent for tasks such as establishing websockets, and obtaining authentication tokens or session information. The AM or load balancer instance can be behind a firewall to which the agent has access.

Define this property when public access to AM is restricted to a different URL from the private URL.

Property name	<code>org.forgerock.agents.public.am.url</code>
Aliases	<code>com.forgerock.agents.public.am.url</code> Introduced in Java Agent 5.6.3.0 <code>org.forgerock.agents.public.am.url</code> Introduced in Java Agent 5.6.3.0
Type	String
Bootstrap property	Yes
Required property	Yes - If this property is missing, the agent fails to start
Restart required	Yes - Restart the container after changing the property
Local configuration file	<code>AgentBootstrap.properties</code>

Response

Response Attribute Map

Map the value of a response attribute specified in AM to one or more HTTP headers, HTTP cookies, or request attributes, depending on the value of Response Attribute Fetch Mode.

- Map key: The name of a response attribute returned by AM with a policy decision
- Map value: The name of one or more HTTP headers, HTTP cookies, or request attributes

Consider the following points for response cookies:

- If an HTTP cookie with the mapped name does not exist, the agent creates it.
- If an HTTP cookie with the mapped name already exists and the cookie value is different from the mapped value, the agent overwrites the cookie.
- If an HTTP cookie with the mapped name already exists and the cookie value is the same as the mapped value, the agent does nothing.
- If the profile attribute name (key) does not exist, the agent does not create the HTTP cookie.
- The agent does not automatically clear cookies. To prevent a build up of cookies, consider adding them to the Reset Cookie List.

Consider the following points for response headers:

- If an HTTP header with the mapped name does not exist, the agent creates it.
- If an HTTP header with the mapped name already exists, the agent does not overwrite it but simply appends information to the HTTP header.
- If the profile attribute name (key) does not exist, the agent does not create the HTTP header.
- When an HTTP header name is used in a request header, it is prefixed by HTTP_ . The agent automatically changes lower case letters to upper case, and hyphens (-) to underscores (_). For example, CUSTOM-userid becomes HTTP_CUSTOM_USERID .

Format: response attribute = HEADER-NAME(S) , response attribute = COOKIE-NAME(S) , response attribute = REQUEST-ATTRIBUTE(S)

Default: Empty

Examples:

In the following example, the AM response attribute uid is mapped to CUSTOM-User-Name: `com.sun.identity.agents.config.response.attribute.mapping[uid]=Custom-User-Name`

Example: `[uid]=HEADER1|HEADER2`

Property name	<code>org.forgerock.agents.response.attribute.map</code>
---------------	--

Aliases	<p><code>org.forgerock.agents.response.attribute.map</code> Introduced in Java Agent 5.6</p> <p><code>com.sun.identity.agents.config.response.attribute.mapping</code> Introduced in Java Agent 5.0 <u>Recognized</u> from AM 6</p>
Type	<p>Map</p> <ul style="list-style-type: none"> • Keys: source response attribute name • Values: one or more target response attribute names
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>
AM console	<p>Tab: Application</p> <p>Title: Response Attribute Map</p> <p>Legacy title: Response Attribute Mapping</p>

Response Attribute Fetch Mode

Map the name of an AM policy response attribute specified in [Response Attribute Map](#) as follows:

- NONE: Do not map
- HTTP_HEADER: Map the to the name of an HTTP response header
- HTTP_COOKIE: Map to the name of an HTTP cookie
- REQUEST_ATTRIBUTE: Map to the name of an HTTP request attribute

Property name	<code>org.forgerock.agents.response.attribute.fetch.mode</code>
---------------	---

Aliases	<p><code>com.sun.identity.agents.config.response.attribute.fetch.mode</code></p> <p>Introduced in Java Agent 5.0 <u>Recognized</u> from AM 6</p> <p><code>org.forgerock.agents.response.attribute.fetch.mode</code></p> <p>Introduced in Java Agent 5.6</p>
Supported settings	<p>NONE No AM attributes are mapped.</p> <p>HTTP_HEADER The named AM attributes are mapped to headers in the outgoing HTTP response.</p> <p>REQUEST_ATTRIBUTE The named AM attributes are mapped to request attributes in the outgoing HTTP response.</p> <p>HTTP_COOKIE The named AM attributes are mapped to cookies in the outgoing HTTP response.</p>
Default	NONE
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>
AM console	<p>Tab: Application</p> <p>Title: Response Attribute Fetch Mode</p>

SSO cookie handling

Enable SSO Token Acceptance

Set this property as follows:

- `true`: Accept SSO tokens. Use this option when the agent and the token issuer are in the same domain, and for web applications and APIs where the backend accepts user

information from SSO tokens.

- `false` : Do not accept SSO tokens; require OIDC JWTs for authentication.

During session upgrade the format of the composite advice is as follows:

- When both this property and Enable Custom Login Mode are `true`, the composite advice has the following format: ?
`authIndexType=composite_advice&authIndexValue=<Advices Value>`
- When either property is `false`, the composite advice has the following format: ?
`composite_advice=<Advices Value>`

Property name	<code>org.forgerock.agents.accept.sso.tokens.enabled</code>
Aliases	<code>org.forgerock.agents.accept.sso.tokens.enabled</code> Introduced in Java Agent 5.7.1 <u>Recognized</u> from AM 7.1 <code>org.forgerock.agents.accept.sso.tokens</code> Introduced in Java Agent 5.7.1 <code>com.forgerock.agents.accept.sso.tokens</code> Introduced in Java Agent 5.7.1
Type	Boolean: <code>true</code> returns true; all other strings return <code>false</code> .
Default	<code>false</code>
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>
AM console	Tab: SSO (from AM 7.1) Title: Enable SSO Token Acceptance Legacy title: Accept SSO Tokens

Convert SSO Tokens Into OIDC JWTs

For each incoming request, the agent looks for an OIDC JWT in the cookie named by JWT Cookie Name. Set this property as follows:

- `true` : Use this value to allow users to access resources protected with systems that continue to use SSO tokens, and to use the default login redirection mode.
 - If the agent does not find a JWT in the cookie, the agent looks for an SSO token in the iPDP cookie defined during AM installation. During agent startup, the agent retrieves the name of this cookie from AM.
 - If the agent finds an SSO token in the iPDP cookie, it makes a request to AM to convert the SSO token into an OIDC JWT.
 - The agent caches the SSO token, so that if it is presented in another incoming request, the agent substitutes the JWT without making a request to AM.
 - If the agent does not find either token, authentication fails. The user can only access resources that are available through not-enforced rules.
- `false` : Do not convert SSO tokens into OIDC JWTs.

Property name	<code>org.forgerock.agents.accept.ipdp.cookie</code>
Aliases	<code>com.forgerock.agents.accept.ipdp.cookie</code> Introduced in Java Agent 5.6 <u>Recognized</u> from AM 7 <code>org.forgerock.agents.accept.ipdp.cookie.enabled</code> Introduced in Java Agent 5.7
Type	Boolean: <code>true</code> returns true; all other strings return <code>false</code> .
Default	<code>false</code>
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>
AM console	Tab: SSO (from AM 7) Title: Convert SSO Tokens Into OIDC JWTs Legacy title: Convert SSO Tokens into OpenID Connect JWTs

SSO Cookie Domain List

When the property `Enable SSO Token Acceptance` is `true`, a list of domains in which the agent attempts to create SSO cookies:

- If the list is empty, the agent creates cookies only in its own domain.
- If the agent is running behind a browser, it can create cookies only in its own domain.
- If the agent is running behind a proxy, it should be able to create cookies in any required domains.

Default: Empty

Property name	<code>org.forgerock.agents.ipdp.cookie.domain.list</code>
Aliases	<code>org.forgerock.agents.ipdp.cookie.domain.list</code> Introduced in Java Agent 5.7.1 <u>Recognized</u> from AM 7.1
Type	List
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>
AM console	Tab: SSO (from AM 7.1) Title: SSO Cookie Domain List

SameSite

Set-Cookie Internal Map

When creating internal cookies, such as `am-auth-jwt` and the pre-authentication cookies, this property sets additional attributes by adding text into the `Set-Cookie` header.

Specify a key:value map, where the key is the cookie name, and the value is the string to add to the `Set-Cookie` header. If the key is omitted, the value becomes the default for all cookies.

Separate multiple values with a semicolon.

Examples:

- Set the SameSite attribute of the am-auth-jwt cookie:
`org.forgerock.agents.set.cookie.internal.map[am-auth-jwt]=samesite=strict`
- Set the SameSite attribute of all cookies:
`org.forgerock.agents.set.cookie.internal.map=samesite=strict`
- Set several attributes of mycookie :
`org.forgerock.agents.set.cookie.internal.map[myCookie]=Max-Age=10000;
Domain=.my.default.fqdn`

Property name	<code>org.forgerock.agents.set.cookie.internal.map</code>
Aliases	<code>org.forgerock.agents.set.cookie.internal.map</code> Introduced in Java Agent 5.6.3.0 <u>Recognized</u> from AM 7
Type	Map <ul style="list-style-type: none">• Keys: Agent internal cookie name• Values: (samesite) text to be added to the Set-Cookie header
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>
AM console	Tab: SSO (from AM 7) Title: Set-Cookie Internal Map

Exclude Agents From Samesite Cookie Attributes

List of user agents excluded from receiving SameSite cookie attributes.

To specify different user agent patterns, add them in AM as custom properties, When user agent patterns are specified, the default list of user agents is ignored.

Property name	<code>org.forgerock.agents.samesite.excluded.user.agents.list</code>
---------------	--

Aliases	<code>org.forgerock.agents.samesite.excluded.user.agents.list</code> Introduced in Java Agent 5.6.3.0 <u>Recognized</u> from AM 7
Type	List
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>
AM console	Tab: SS0 (from AM 7) Title: Exclude Agents From Samesite Cookie Attributes Legacy title: Samesite Cookie Attributes Excluded User Agents Pattern List

Set-Cookie Attribute Map

When creating cookies with the `AttributeTaskHandler`, this property sets additional attributes by adding text into the `Set-Cookie` header.

Specify a key:value map, where the key is the cookie name, and the value the string to add to the the `Set-Cookie` header.

Separate multiple values with a semicolon.

Property name	<code>org.forgerock.agents.set.cookie.attribute.map</code>
Aliases	<code>org.forgerock.agents.set.cookie.attribute.map</code> Introduced in Java Agent 5.6.3.0 <u>Recognized</u> from AM 7
Type	Map <ul style="list-style-type: none"> • Keys: Cookie name • Values: (samesite) text to be added to the Set-Cookie header

Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	AgentConfig.properties
AM console	Tab: SSO (from AM 7) Title: Set-Cookie Attribute Map

Session

Session Attribute Fetch Mode

Map the name of an AM session attribute specified in [Session Attribute Map](#) as follows:

- NONE: Do not map
- HTTP_HEADER: Map the to the name of an HTTP session header
- HTTP_COOKIE: Map to the name of an HTTP cookie
- REQUEST_ATTRIBUTE: Map to the name of an HTTP session attribute

When the value is HTTP_COOKIE , [Cookie Reset](#) is automatically set to true . Before redirecting the client for login, and when the client logs out, the agent resets profile and session attributes cookies, and cookies in the [Reset Cookie List](#).

Property name	org.forgerock.agents.session.attribute.fetch.mode
Aliases	org.forgerock.agents.session.attribute.fetch.mode Introduced in Java Agent 5.6 com.sun.identity.agents.config.session.attribute.fetch.mode Introduced in Java Agent 5.0 Recognized from AM 6

Supported settings	<p>NONE No AM attributes are mapped.</p> <p>HTTP_HEADER The named AM attributes are mapped to headers in the outgoing HTTP response.</p> <p>REQUEST_ATTRIBUTE The named AM attributes are mapped to request attributes in the outgoing HTTP response.</p> <p>HTTP_COOKIE The named AM attributes are mapped to cookies in the outgoing HTTP response.</p>
Default	NONE
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	AgentConfig.properties
AM console	<p>Tab: Application</p> <p>Title: Session Attribute Fetch Mode</p>

Session Attribute Map

Map the value of an AM session attribute to one or more HTTP headers, HTTP cookies, or request attributes, depending on the value of Session Attribute Fetch Mode. The session attribute is the attribute in the session to be fetched.

- Map key: The name of an AM session attribute
- Map value: The name of one or more HTTP headers, HTTP cookies, or request attributes

Consider the following points for HTTP cookies:

- If an HTTP cookie with the mapped name does not exist, the agent creates it.
- If an HTTP cookie with the mapped name already exists and the cookie value is different from the mapped value, the agent overwrites the cookie.

- If an HTTP cookie with the mapped name already exists and the cookie value is the same as the mapped value, the agent does nothing.
- If the profile attribute name (key) does not exist, the agent does not create the HTTP cookie.
- The agent does not automatically clear cookies. To prevent a build up of cookies, consider adding them to the [Reset Cookie List](#).

Consider the following points for HTTP headers:

- If an HTTP header with the mapped name does not exist, the agent creates it.
- If an HTTP header with the mapped name already exists, the agent does not overwrite it but simply appends information to the header.
- If the profile attribute name (key) does not exist, the agent does not create the response header.
- When an HTTP header name is used in a request header, it is prefixed by HTTP_ . The agent automatically changes lower case letters to upper case, and hyphens (-) to underscores (_). For example, CUSTOM-userid becomes HTTP_CUSTOM_USERID .

Format: session attribute = HEADER-NAME(S) , session attribute = COOKIE-NAME(S) , session attribute = REQUEST-ATTRIBUTE(S)

Default: Empty

Examples:

In the following example, the AM response attribute uid is mapped to CUSTOM-User-Name: `com.sun.identity.agents.config.response.attribute.mapping[uid]=Custom-User-Name`

Example: `[UserToken]=HEADER-1|HEADER-2`

Property name	<code>org.forgerock.agents.session.attribute.map</code>
Aliases	<code>org.forgerock.agents.session.attribute.map</code> Introduced in Java Agent 5.6 <code>com.sun.identity.agents.config.session.attribute.mapping</code> Introduced in Java Agent 5.0 <u>Recognized</u> from AM 6
Type	Map <ul style="list-style-type: none"> • Keys: source session attribute name • Values: one or more target session attribute names

Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	AgentConfig.properties
AM console	Tab: Application Title: Session Attribute Map Legacy title: Session Attribute Mapping

Session Cache TTL

The interval in minutes at which entries in the session cache timeout and are purged.

If an entry is not cached, the agent must retrieve session information from AM. Therefore, by default the timeout is much longer than for the policy cache.

Property name	<code>org.forgerock.agents.session.cache.ttl.minutes</code>
Aliases	<code>org.forgerock.agents.session.cache.ttl.minutes</code> Introduced in Java Agent 5.6 <code>org.forgerock.openam.agents.config.active.session.cache.ttl.minutes</code> Introduced in Java Agent 5.0 <u>Recognized</u> from AM 7
Type	Integer
Default	15
Bootstrap property	Yes
Required property	No
Restart required	Yes - Restart the container after changing the property
Local configuration file	AgentBootstrap.properties
AM console	Tab: Advanced (from AM 7) Title: Session Cache TTL

Max Entries in Expired Session Cache

The maximum number of entries in the expired session cache. When the maximum is reached, the oldest records are overwritten.

Property name	<code>org.forgerock.agents.expired.session.cache.size</code>
Aliases	<code>org.forgerock.agents.expired.session.cache.size</code> Introduced in Java Agent 5.7.1 <u>Recognized</u> from AM 7.1
Type	Integer
Default	500
Bootstrap property	Yes
Required property	No
Restart required	Yes - Restart the container after changing the property
Local configuration file	<code>AgentBootstrap.properties</code>
AM console	Tab: Advanced (from AM 7.1) Title: Max Entries in Expired Session Cache Legacy title: Expired Session Cache Max Records

Expired Session Cache Timeout

The interval in minutes at which entries in the expired session cache timeout and are purged.

The expired session cache records sessions that have been killed by AM. Use the cache to reduce network traffic and load on AM. When the agent receives a request using an invalidated token, it rejects the request without requesting session information from AM.

Property name	<code>org.forgerock.agents.sso.expired.session.cache.ttl.minutes</code>
Aliases	<code>org.forgerock.agents.sso.expired.session.cache.ttl.minutes</code> Introduced in Java Agent 5.7.1 <u>Recognized</u> from AM 7.1

Type	Integer
Default	20
Bootstrap property	Yes
Required property	No
Restart required	Yes - Restart the container after changing the property
Local configuration file	AgentBootstrap.properties
AM console	Tab: Advanced (from AM 7.1) Title: Expired Session Cache Timeout

Timeout

Websocket Idle Timeout

The idle timeout in milliseconds for WebSockets. If the connection is not active for this time, the agent pings AM to keep the WebSocket alive.

Property name	<code>org.forgerock.agents.ping.websocket.after.inactive.milliseconds</code>
Aliases	<code>org.forgerock.agents.ping.websocket.after.inactive.milliseconds</code> Introduced in Java Agent 5.8
Type	Integer
Default	20000
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	AgentConfig.properties

Websocket Expired Timeout

The allowed ping response time in milliseconds for WebSockets. If the WebSocket does not respond to a ping within this time, the agent closes the connection.

Property name	<code>org.forgerock.agents.declare.websocket.dead.after.milliseconds</code>
Aliases	<code>org.forgerock.agents.declare.websocket.dead.after.milliseconds</code> Introduced in Java Agent 5.8
Type	Integer
Default	40000
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>

User mapping

User Attribute Name

When the property `User Mapping Mode` is `HTTP_HEADER`, this property is the name of the HTTP header attribute to identify the user. The named header must be present in the incoming headers.

Property name	<code>org.forgerock.agents.user.mapping.mode.attribute.name</code>
Aliases	<code>com.sun.identity.agents.config.user.attribute.name</code> Introduced in Java Agent 5.0 <u>Recognized</u> from AM 6 <code>org.forgerock.agents.user.mapping.mode.attribute.name</code> Introduced in Java Agent 5.6
Type	String
Default	<code>employeenumber</code>

Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	AgentConfig.properties
AM console	Tab: Global Title: User Attribute Name

User Mapping Mode

Specifies where to obtain the user ID

Property name	<code>org.forgerock.agents.user.mapping.mode</code>
Aliases	<code>org.forgerock.agents.user.mapping.mode</code> Introduced in Java Agent 5.6 <code>com.sun.identity.agents.config.user.mapping.mode</code> Introduced in Java Agent 5.0 <u>Recognized</u> from AM 6

Supported settings	<p>USER_ID</p> <p>If "Enable User Principal Flag" (org.forgerock.agents.userid.mapping.mode.use.dn.enabled) is true, the user ID is set from the User Principal. Otherwise, the user ID is set from the user's session property nominated by "User Session Name" (org.forgerock.agents.userid.mapping.mode.use.session.property.name).</p> <p>PROFILE_ATTRIBUTE</p> <p>The user ID is set to the value of a named profile attribute specified by "User Attribute Name" (org.forgerock.agents.user.mapping.mode.attribute.name).</p> <p>HTTP_HEADER</p> <p>The user ID is set to the value of the HTTP header specified by the "User Attribute Name" (org.forgerock.agents.user.mapping.mode.attribute.name).</p> <p>SESSION_PROPERTY</p> <p>The user ID is set to the value of the session property specified by the "User Attribute Name" (org.forgerock.agents.user.mapping.mode.attribute.name).</p>
Default	USER_ID
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	AgentConfig.properties
AM console	<p>Tab: Global</p> <p>Title: User Mapping Mode</p>

User Session Name

The user is identified by the value of this property when User Mapping Mode is `USER_ID`, and Enable User Principal Flag is `false`.

Property name	org.forgerock.agents.userid.mapping.mode.use.session.property.name
Aliases	com.sun.identity.agents.config.user.token Introduced in Java Agent 5.0 <u>Recognized</u> from AM 6 org.forgerock.agents.userid.mapping.mode.use.session.property.name Introduced in Java Agent 5.6
Type	String
Default	UserToken
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	AgentConfig.properties
AM console	Tab: Global Title: User Session Name Legacy title: User Token Name

Enable User Principal Flag

When the property User Mapping Mode is `USER_ID`, this flag indicates whether to identify the user through the user DN, as follows:

- If `true`, the DN is taken from `universalId`, retrieved from the AM user session info.
- If `false`, the user is identified by the the property User Session Name.

Property name	org.forgerock.agents.userid.mapping.mode.use.dn.enabled
---------------	---

Aliases	<p><code>com.sun.identity.agents.config.user.principal</code> Introduced in Java Agent 5.0 <u>Recognized</u> from AM 6</p> <p><code>org.forgerock.agents.userid.mapping.mode.use.dn.enabled</code> Introduced in Java Agent 5.6</p>
Type	Boolean: true returns true; all other strings return false.
Default	false
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>
AM console	<p>Tab: Global</p> <p>Title: Enable User Principal Flag</p> <p>Legacy title: User Principal Flag</p>