

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.

Aliases starting with `org.forgerock` follow a naming convention to provide information about the property.

When a property has multiple aliases, the agent evaluates the aliases in alphabetical order. If the aliases each specify 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
```

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](#)
- [Encrypting Java class](#)
- [Encryption Digest](#)
- [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](#)
- [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 Cache](#)
- [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 Size](#)
- [POST Data Preservation Cache TTL](#)
- [POST Data Preservation Cache TTL in Milliseconds \(deprecated\)](#)
- [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 URI

- [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](#)

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](#)
- [Encrypting Java class](#)
- [AM Authentication Service Protocol](#)
- [AM Authentication Service Host Name](#)
- [AM Authentication Service Port](#)
- [Encryption Key](#)
- [Encryption Digest](#)

Client Identification

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

Common Attributes Fetching

- [Cookie Separator Character](#)
- [Fetch Attribute Date Format](#)
- [Enable Attribute Encoding](#)

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

- [Max Age of Pre-Authentication Cookie](#)
- [Load Balancer Cookie Name](#)
- [Enable Encoded Cookies](#)
- [Enable HTTP Only Cookies](#)
- [Pre-Authentication Cookie Name](#)
- [Enable Load Balancer Cookies](#)

Cookie Reset

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

- [Reset Cookie Path Map](#)

Cross-Domain Single Sign-On

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

Cross-Site Scripting

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

Debug and Metric

- [Debug File Rotation Size](#)
- [Debug File Rotation Suffix](#)
- [Agent Debug Level](#)
- [Debug File Rotation Retention Count](#)
- [Debug File Rotation Time](#)
- [Debug File Rotation Prefix](#)

Fragment Relay

- [Fragment Relay URI](#)

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 URL

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

Logout

- [Logout URI Map](#)
- [Logout Request Parameter Map](#)
- [Enable Logout Introspection](#)

- [Logout Entry URI Map](#)

Logs

- [Log File Directory](#)

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

- [Java Class for Matching Not Enforced Rules](#)

Not-Enforced

- [Enable Not-Enforced IP Cache](#)
- [Not-Enforced URIs](#)
- [Invert Not-Enforced IPs](#)
- [Not-Enforced Client IP List](#)
- [Not-Enforced Favicon](#)
- [Enable Not-Enforced URIs Cache](#)
- [Max Entries in Not-Enforced IP Cache](#)
- [Not-Enforced Compound Rule Separator](#)
- [Invert Not-Enforced URIs](#)
- [Max Entries in Not-Enforced URI Cache](#)

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 Sticky Session Mode](#)
- [Enable POST Data Preservation](#)
- [Missing POST Data Preservation Entry URI Map](#)
- [POST Data Preservation Cache Size](#)
- [Max Entries in POST Data Preservation Cache](#)
- [POST Data Preservation Cache TTL](#)
- [POST Data Preservation Sticky Session Key Value](#)
- [POST Data Preservation Cache TTL in Milliseconds \(deprecated\)](#)

Policy Client Service

- [Session Cache TTL](#)
- [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 \(deprecated\)](#)

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 Handling

- [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](#)
- [AM Authentication Service Protocol](#)
- [Encrypted Agent Password](#)
- [Location of Agent Configuration Repository](#)
- [Public AM URL](#)

- [Authentication Redirect URI](#)
- [Encrypting Java class](#)
- [Agent Profile Realm](#)
- [Agent Profile Name](#)
- [Autonomous mode](#)
- [AM Authentication Service Host Name](#)
- [AM Authentication Service Port](#)
- [Encryption Key](#)

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](#)

Session

- [Session Attribute Fetch Mode](#)
- [Session Attribute Map](#)
- [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 URI

Access Denied URI Map

Resource Access Denied URI

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>
Property aliases	<code>com.sun.identity.agents.config.access.denied.uri</code> (since 5.0) <code>org.forgerock.agents.access.denied.uri.map</code> (since 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	<i>Application</i>

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>
Property aliases	<code>com.sun.identity.agents.config.agent.protocol</code> (since 5.0) <code>org.forgerock.agents.agent.protocol</code> (since 5.6)
Type	String
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>
AM console tab	<i>Advanced</i>

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>
---------------	---

Property aliases	<p><code>com.forgerock.agents.config.fallback.mode</code> (since 5.9.0)</p> <p><code>org.forgerock.agents.fallback.mode.enabled</code> (since 5.9.0)</p> <p><code>org.forgerock.agents.autonomous.mode.enabled</code> (since 5.9.0)</p>
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>
Property aliases	<code>org.forgerock.agents.am.unavailability.recheck.window.in.seconds</code> (since 5.9.0)
Type	Integer
Default	5
Bootstrap property	No

Required property	No
Restart required	No
Local configuration file	AgentConfig.properties

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
Property aliases	com.sun.identity.agents.config.agent.port (since 5.0) org.forgerock.agents.agent.port (since 5.6)
Type	Integer
Default	''
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	AgentConfig.properties
AM console tab	<i>Advanced</i>

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>
Property aliases	<code>com.sun.identity.agents.config.agent.host</code> (since 5.0) <code>org.forgerock.agents.agent.hostname</code> (since 5.6)
Type	String
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>
AM console tab	<i>Advanced</i>

Agent Filter Mode Map

Agent Filter Mode

The operation mode of the agent filter.

Property name	<code>org.forgerock.agents.filter.mode.map</code>
Property aliases	<code>com.sun.identity.agents.config.filter.mode</code> (since 5.0) <code>org.forgerock.agents.filter.mode.map</code> (since 5.6.2.1)

Supported settings	<p><i>NONE</i> The agent performs no authentication check, and any resource access request is granted.</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	URL_POLICY
Bootstrap property	Yes
Required property	No
Restart required	No
Local configuration file	AgentBootstrap.properties
AM console tab	<i>Global</i>

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>
Property aliases	<code>org.forgerock.agents.strategy.when.am.unavailable</code> (since 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

Audit

Enable Local Audit Log Rotation

Rotate Local Audit Log

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>
Property aliases	<p><code>org.forgerock.agents.local.audit.log.rotation.enabled</code> (since 5.6)</p> <p><code>com.sun.identity.agents.config.local.log.rotate</code> (since 5.0)</p>
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	<i>Global</i>

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>
Property aliases	<code>com.sun.identity.agents.config.local.log.size</code> (since 5.0) <code>org.forgerock.agents.local.audit.log.rotation.bytes</code> (since 5.7)
Type	Integer
Default	52428800
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	AgentConfig.properties
AM console tab	<i>Global</i>

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>
Property aliases	<code>org.forgerock.agents.local.audit.log.retention.count</code> (since 5.7)
Type	Integer
Default	-1
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>
AM console tab	<i>Global</i>

Audit Access Types

The type of messages to audit.

Property name	<code>org.forgerock.agents.audit.what</code>
Property aliases	<code>com.sun.identity.agents.config.audit.accesstype</code> (since 5.0) <code>org.forgerock.agents.audit.what</code> (since 5.6)
Supported settings	<p><i>LOG_NONE</i> Don't audit anything.</p> <p><i>LOG_ALLOW</i> Audit only allowed requests.</p> <p><i>LOG_DENY</i> Audit only denied requests.</p> <p><i>LOG_BOTH</i> Audit both allowed and denied requests.</p>
Default	<code>LOG_NONE</code>
Bootstrap property	No

Required property	No
Restart required	No
Local configuration file	AgentConfig.properties
AM console tab	<i>Global</i>

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
Property aliases	com.sun.identity.agents.config.local.logfile (since 5.0) org.forgerock.agents.local.audit.file.path (since 5.6)
Type	String
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	AgentConfig.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
Property aliases	com.sun.identity.agents.config.log.disposition (since 5.0) org.forgerock.agents.audit.where (since 5.6)

Supported settings	<p>NONE Don't audit anything, anywhere.</p> <p>LOCAL Audit locally only.</p> <p>REMOTE Audit remotely only.</p> <p>ALL Audit both locally and remotely.</p>
Default	NONE
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	AgentConfig.properties
AM console tab	Global

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	org.forgerock.agents.authn.fail.reason.parameter.name
Property aliases	org.forgerock.agents.authn.fail.reason.parameter.name (since 5.7)
Type	String

Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	AgentConfig.properties
AM console tab	Miscellaneous

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	<code>org.forgerock.agents.authn.fail.reason.remapper</code>
Property aliases	<code>org.forgerock.agents.authn.fail.reason.remapper</code> (since 5.7)
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	<code>AgentConfig.properties</code>
AM console tab	<i>Miscellaneous</i>

Authentication Fail URL

Authentication Fail Reason 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 both are unset, the agent returns HTTP status 400.

To configure the agent to send the reason for authentication failure in a query parameter, configure Authentication Fail Reason Parameter Name.

Property name	<code>org.forgerock.agents.authn.fail.url</code>
Property aliases	<code>org.forgerock.agents.authn.fail.url</code> (since 5.7)
Type	String
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>
AM console tab	<i>Miscellaneous</i>

Goto URL

The URL to which the agent redirects when related properties are not set.

For example, after an authentication failure, if Authentication Fail Reason Parameter Name is not set, the agent redirects to the value of this property.

Property name	<code>org.forgerock.agents.default.goto.url</code>
Property aliases	<code>com.sun.identity.agents.config.openam.agent.default_goto_url</code> (since 5.0) <code>org.forgerock.agents.default.goto.url</code> (since 5.7)
Type	String
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>
AM console tab	<i>Miscellaneous</i>

Authentication Service

AM Authentication Service Path

The path to the AM server.

Property name	<code>org.forgerock.agents.am.path</code>
Property aliases	<code>com.ipplanet.am.services.deploymentDescriptor</code> (since 5.0) <code>org.forgerock.agents.am.path</code> (since 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>

Encrypting Java class

The Java class used to encrypt the agent password.

During installation, the class is set in the bootstrap properties file with the default value. Change the class only to reduce your level of encryption.

To change the class, make sure that the class is available at runtime, regenerate the agent password using the agent installer, and manually edit the newly generated encrypted password into the bootstrap properties file.

Property name	<code>org.forgerock.agents.encryptor.classname</code>
Property aliases	<code>org.forgerock.agents.encryptor.classname</code> (since 5.7) <code>com.ipplanet.security.encryptor</code> (since 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	Yes - Restart the container after changing the property
Local configuration file	AgentBootstrap.properties

AM Authentication Service Protocol

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

- HTTP
- HTTPS

Property name	org.forgerock.agents.am.protocol
Property aliases	org.forgerock.agents.am.protocol (since 5.6) com.ipplanet.am.server.protocol (since 5.0)
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
AM console tab	<i>AM Services</i>

AM Authentication Service Host Name

The AM server host name.

Property name	org.forgerock.agents.am.hostname
Property aliases	com.ipplanet.am.server.host (since 5.0) org.forgerock.agents.am.hostname (since 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	AgentBootstrap.properties
AM console tab	AM Services

AM Authentication Service Port

The AM server port number.

Property name	org.forgerock.agents.am.port
Property aliases	com.ip1anet.am.server.port (since 5.0) org.forgerock.agents.am.port (since 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	AgentBootstrap.properties
AM console tab	AM Services

Encryption Key

The key with which to encrypt the agent password.

The key is set during installation process. To change it after installation:

- Manually invoke `agentadmin` with the `--getEncryptKey` option
- Manually edit the result into the bootstrap property file, against the encryption key property
- Re-encrypt your password using `agentadmin` with the `--encrypt` option
- Manually edit the encrypted result into the bootstrap property file, against the encrypted password property

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

Property name	<code>am.encryption.pwd</code>
Property aliases	<code>am.encryption.pwd</code> (since 5.0)
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>AgentKey.properties</code>

Encryption Digest

The hashing algorithm used internally by the agent.

Changing this property it is not recommended, because it can cause the agent to fail randomly.

Property name	<code>org.forgerock.agents.encryption.key.digest</code>
Property aliases	<code>org.forgerock.openam.encryption.key.digest</code> (since 5.0) <code>org.forgerock.agents.encryption.key.digest</code> (since 5.6)
Type	String
Default	SHA256
Bootstrap property	Yes
Required property	No
Restart required	Yes - Restart the container after changing the property
Local configuration file	<code>AgentBootstrap.properties</code>

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>
Property aliases	<code>org.forgerock.agents.http.header.containing.remote.hostname</code> (since 5.6) <code>com.sun.identity.agents.config.client.hostname.header</code> (since 5.0)
Type	String
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>
AM console tab	<i>Advanced</i>

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>
Property aliases	<code>org.forgerock.agents.original.ip.check.mode.map</code> (since 5.8.0)

Supported settings	<p>OFF IP address checking is disabled.</p> <p>DENY An "unacceptable" IP address change triggers an HTTP 403 response.</p> <p>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.</p>
Default	OFF
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	AgentConfig.properties
AM console tab	<i>Application</i>

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	org.forgerock.agents.acceptable.ip.address.map
Property aliases	org.forgerock.agents.acceptable.ip.address.map (since 5.8.0)
Type	<p>Map</p> <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	AgentConfig.properties
AM console tab	<i>Application</i>

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>
Property aliases	<code>com.sun.identity.agents.config.client.ip.header</code> (since 5.0) <code>org.forgerock.agents.http.header.containing.ip.address</code> (since 5.6)
Type	String
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	AgentConfig.properties
AM console tab	<i>Advanced</i>

Common Attributes Fetching

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>
Property aliases	<code>com.sun.identity.agents.config.attribute.cookie.separator</code> (since 5.0) <code>org.forgerock.agents.attribute.cookie.separator</code> (since 5.6)
Type	String
Default	
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>
AM console tab	<i>Application</i>

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>
Property aliases	<code>com.sun.identity.agents.config.attribute.date.format</code> (since 5.0) <code>org.forgerock.agents.attribute.date.format</code> (since 5.6)
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	<code>AgentConfig.properties</code>

AM console tab

Application

Enable Attribute Encoding

Attribute Cookie Encode

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

Property name	<code>org.forgerock.agents.attribute.cookie.encode.enabled</code>
Property aliases	<code>com.sun.identity.agents.config.attribute.cookie.encode</code> (since 5.0) <code>org.forgerock.agents.attribute.cookie.encode.enabled</code> (since 5.6)
Type	Boolean: <code>true</code> returns <code>true</code> ; 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>
AM console tab	<i>Application</i>

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>
Property aliases	<code>org.forgerock.agents.http.client.max.connections</code> (since 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	<i>Redirect</i>

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>
Property aliases	<code>org.forgerock.agents.http.client.connection.timeout.seconds</code> (since 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	AgentBootstrap.properties
AM console tab	<i>Redirect</i>

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>
Property aliases	<code>org.forgerock.agents.http.client.reuse.connections.enabled</code> (since 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>

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>
Property aliases	<code>org.forgerock.agents.http.client.connection.state.enabled</code> (since 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>
Property aliases	<code>org.forgerock.agents.use.connection.pooling.enabled</code> (since 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	AgentConfig.properties

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>
Property aliases	<code>org.forgerock.agents.http.client.socket.timeout.seconds</code> (since 5.8.0)

Type	Integer
Default	0
Bootstrap property	Yes
Required property	No
Restart required	Yes - Restart the container after changing the property
Local configuration file	AgentBootstrap.properties

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>
Property aliases	<code>org.forgerock.agents.http.client.retry.requests.enabled</code> (since 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

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>
Property aliases	<code>org.forgerock.agents.container.encoding</code> (since 5.9.1)
Type	String
Default	UTF-8
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>

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>
Property aliases	<code>org.forgerock.agents.container.param.encoding</code> (since 5.9.1)
Type	String
Default	ISO-8859-1
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>

Continuous Security

Continuous Security Cookie Map

Continuous Security Cookies

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	<code>org.forgerock.agents.continuous.security.cookies.map</code>
Property aliases	<code>org.forgerock.agents.continuous.security.cookies.map</code> (since 5.6) <code>org.forgerock.openam.agents.config.continuous.security.cookies</code> (since 5.0)
Type	Map <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 tab	<i>Application</i>

Continuous Security Header Map

Continuous Security Headers

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>
---------------	---

Property aliases	<p><code>org.forgerock.agents.continuous.security.headers.map</code> (since 5.6)</p> <p><code>org.forgerock.openam.agents.config.continuous.security.headers</code> (since 5.0)</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 tab	<i>Application</i>

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>
Property aliases	<p><code>org.forgerock.agents.http.header.containing.remote.hostname</code> (since 5.6)</p> <p><code>com.sun.identity.agents.config.client.hostname.header</code> (since 5.0)</p>
Type	String
Bootstrap property	No
Required property	No
Restart required	No

Local configuration file	AgentConfig.properties
AM console tab	<i>Advanced</i>

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>
Property aliases	<code>com.sun.identity.agents.config.client.ip.header</code> (since 5.0) <code>org.forgerock.agents.http.header.containing.ip.address</code> (since 5.6)
Type	String
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	AgentConfig.properties
AM console tab	<i>Advanced</i>

Cookie

Max Age of Pre-Authentication Cookie

Pre-Authenticated Cookie Max Age

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>
Property aliases	<code>org.forgerock.agents.authn.cookie.max.age.seconds</code> (since 5.6.3.0)
Type	Integer
Default	300
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>
AM console tab	<i>Global</i>

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>
Property aliases	<code>org.forgerock.agents.load balancer.cookie.name</code> (since 5.8.0)
Type	String
Default	<code>amlbcookie</code>
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>
AM console tab	<i>Global</i>

Enable Encoded Cookies

Encode Cookies

When `true`, cookies are base64-encoded.

Property name	<code>com.ipplanet.am.cookie.encode</code>
Property aliases	<code>com.ipplanet.am.cookie.encode</code> (since 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	<i>SSO</i>

Enable HTTP Only Cookies

Http Only

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

Property name	<code>com.sun.identity.cookie.httponly</code>
Property aliases	<code>com.sun.identity.cookie.httponly</code> (since 5.0)
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	SSO

Pre-Authentication Cookie Name

Pre-Authenticated 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>
Property aliases	<code>com.sun.identity.agents.config.cdsso.cookie.name</code> (since 5.0) <code>org.forgerock.agents.authn.cookie.name</code> (since 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	<i>Global</i>

Enable Load Balancer Cookies

Load Balancer Cookie Enabled

When `true`, the agent writes load balancer cookies each time AM is invoked.

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).

Property name	<code>org.forgerock.agents.load.balancer.cookies.enabled</code>
Property aliases	<code>org.forgerock.agents.load.balancer.cookies.enabled</code> (since 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	AgentConfig.properties
AM console tab	<i>Global</i>

Cookie Reset

Reset Cookie List

Cookies Reset Name List

List of cookies to reset if Cookie Reset is `true`.

The agent searches for the cookie name using a case-sensitive search. If a match is found, the cookie is returned. If the match fails, the agent searches again, using a case-insensitive search. If a match is found the cookie is returned, and a warning is issued to the logs.

Property name	<code>org.forgerock.agents.cookie.reset.name.list</code>
Property aliases	<code>org.forgerock.agents.cookie.reset.name.list</code> (since 5.6) <code>com.sun.identity.agents.config.cookie.reset.name</code> (since 5.0)
Type	List
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	AgentConfig.properties
AM console tab	<i>SSO</i>

Cookie Reset

When `true`, the agent resets cookies in the response before redirecting to authentication.

When Profile Attribute Fetch Mode or Session Attribute Fetch Mode has the value `HTTP_COOKIE`, the agent builds a list of cookies.

Property name	<code>org.forgerock.agents.cookie.reset.enabled</code>
Property aliases	<code>org.forgerock.agents.cookie.reset.enabled</code> (since 5.6) <code>com.sun.identity.agents.config.cookie.reset.enable</code> (since 5.0)
Type	Boolean: <code>true</code> returns true; all other strings return false.
Default	<code>false</code>
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>
AM console tab	<i>SSO</i>

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 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>
Property aliases	<code>org.forgerock.agents.set.cookie.internal.map</code> (since 5.6.3.0)
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

Exclude Agents From Samesite Cookie Attributes

Samesite Cookie Attributes Excluded User Agents Pattern List

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>
Property aliases	<code>org.forgerock.agents.samesite.excluded.user.agents.list</code> (since 5.6.3.0)
Type	List
Bootstrap property	No

Required property	No
Restart required	No
Local configuration file	AgentConfig.properties
AM console tab	SSO

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>
Property aliases	<code>org.forgerock.agents.set.cookie.attribute.map</code> (since 5.6.3.0)
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

Reset Cookie Domain Map

Cookies Reset Domain Map

Specifies how names from [Reset Cookie List](#) correspond to cookie domain values when the cookie is reset.

Property name	<code>org.forgerock.agents.cookie.reset.domain.map</code>
Property aliases	<code>org.forgerock.agents.cookie.reset.domain.map</code> (since 5.6) <code>com.sun.identity.agents.config.cookie.reset.domain</code> (since 5.0)
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	<code>AgentConfig.properties</code>
AM console tab	<i>SSO</i>

Reset Cookie Path Map

Cookies Reset Path Map

Specifies how names from [Reset Cookie List](#) correspond to cookie paths when the cookie is reset.

Property name	<code>org.forgerock.agents.cookie.reset.path.map</code>
Property aliases	<code>com.sun.identity.agents.config.cookie.reset.path</code> (since 5.0) <code>org.forgerock.agents.cookie.reset.path.map</code> (since 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	SSO

Cross-Domain Single Sign-On

Transmit Cookies Securely

CDSSO Secure Enable

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>
Property aliases	<code>com.sun.identity.agents.config.cdsso.secure.enable</code> (since 5.0) <code>org.forgerock.agents.secure.cookies.enabled</code> (since 5.6) <code>com.ipplanet.am.cookie.secure</code> (since 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

Authentication Redirect URI

CSSO 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>
Property aliases	<code>org.forgerock.agents.authn.redirect.uri</code> (since 5.6) <code>com.sun.identity.agents.config.cdsso.redirect.uri</code> (since 5.0)
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	<i>SSO</i>

Cross-Site Scripting

XSS Code Element List

Possible XSS code elements

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>
---------------	---

Property aliases	org.forgerock.agents.xss.code.element.list (since 5.7) com.sun.identity.agents.config.xss.code.elements (since 5.0)
Type	List
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	AgentConfig.properties
AM console tab	<i>Advanced</i>

XSS Redirect URI Map

XSS detection redirect URI

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	org.forgerock.agents.xss.redirect.uri.map
Property aliases	com.sun.identity.agents.config.xss.redirect.uri (since 5.0) org.forgerock.agents.xss.redirect.uri.map (since 5.7)
Type	Map <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	AgentConfig.properties
AM console tab	<i>Advanced</i>

Debug and Metric

Debug File Rotation Size

The approximate size in bytes at which a log file is rotated to a new log file. To enable file rotation, set this property and [Debug File Rotation Time](#).

When the value is `-1`, file rotation is disabled.

Property name	<code>org.forgerock.agents.debug.rotation.size.bytes</code>
Property aliases	<code>org.forgerock.agents.debug.rotation.size.bytes</code> (since 5.7) <code>org.forgerock.openam.debug.rotation.maxsize</code> (since 5.0)
Type	Integer
Default	<code>-1</code>
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	AgentConfig.properties
AM console tab	<i>Global</i>

Debug File Rotation Suffix

When the properties [Debug File Rotation Size](#) and [Debug File Rotation Time](#) are set, log rotation is enabled, and this suffix is appended to the end of the log file name when it is rotated. If log rotation is disabled, nothing is appended to the log file name.

The suffix can be defined freely, however, if it does not include a timestamp that produces different file names when the rotation time is reached, log file rotation can fail. Invalid values produce exceptions in the container logs or agent logs.

For information about how to configure this property, see the `java.text.SimpleDateFormat` Java class in the Java SDK documentation.

Default: `-yyyy.MM.dd-HH.mm`

Property name	<code>org.forgerock.agents.debug.suffix</code>
Property aliases	<code>org.forgerock.openam.debug.suffix</code> (since 5.0) <code>org.forgerock.agents.debug.suffix</code> (since 5.7)
Type	String
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>
AM console tab	<i>Global</i>

Agent Debug Level

Specifies the agent debugging level.

Not all containers capture all messages logged to the standard output, and warnings or critical errors can easily disappear forever.

Property name	<code>org.forgerock.agents.debug.level</code>
Property aliases	<code>com.ipplanet.services.debug.level</code> (since 5.0) <code>org.forgerock.agents.debug.level</code> (since 5.6)

Supported settings	<p>OFF No logging is performed, except for critical errors which cannot be disabled.</p> <p>ERROR Only errors are logged.</p> <p>WARNING Only errors and warnings are logged.</p> <p>MESSAGE Errors, warnings, and informative messages are logged.</p> <p>TRACE The highest level of logging available. Do not use for long periods in production environments.</p> <p>ON The highest level of logging. Logs are written to the standard output instead of to a log file. Your container must be able to cope with this.</p>
Default	ERROR
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	AgentConfig.properties
AM console tab	Global

Debug File Rotation Retention Count

The number of debug 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.debug.retention.count</code>
---------------	---

Property aliases	<code>org.forgerock.agents.debug.retention.count</code> (since 5.7)
Type	Integer
Default	-1
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>
AM console tab	<i>Global</i>

Debug File Rotation Time

The time in minutes, after which a log file is rotated to a new log file. To enable file rotation, set this property and [Debug File Rotation Size](#).

When the value is `-1`, file rotation is disabled.

Property name	<code>org.forgerock.agents.debug.rotation.time.minutes</code>
Property aliases	<code>org.forgerock.openam.debug.rotation</code> (since 5.0) <code>org.forgerock.agents.debug.rotation.time.minutes</code> (since 5.7)
Type	Integer
Default	-1
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>

Debug File Rotation Prefix

A prefix to append to the start of the log file name. See also [Debug File Rotation Suffix](#).

Default: Empty

Property name	<code>org.forgerock.agents.debug.prefix</code>
Property aliases	<code>org.forgerock.openam.debug.prefix</code> (since 5.0) <code>org.forgerock.agents.debug.prefix</code> (since 5.7)
Type	String
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>
AM console tab	<i>Global</i>

Fragment Relay

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>
Property aliases	<code>org.forgerock.agents.authn.fragment.relay.uri</code> (since 5.7)
Type	String

Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	AgentConfig.properties
AM console tab	<i>Advanced</i>

Fully Qualified Domain Name

Default FQDN

FQDN Default

The default FQDN to use for the incoming server, if the agent cannot find a value in the FQDN map. If this property is not defined, FQDN checking is disabled.

This property ensures that when users access protected resources on the web server without specifying the FQDN, the agent can redirect the users to URLs containing the correct FQDN.

Property name	org.forgerock.agents.fqdn.default
Property aliases	org.forgerock.agents.fqdn.default (since 5.6) com.sun.identity.agents.config.fqdn.default (since 5.0)
Type	String
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	AgentConfig.properties
AM console tab	<i>Global</i>

FQDN Map

FQDN Virtual Host Map

A case-insensitive map of invalid server names to valid server names.

Property name	<code>org.forgerock.agents.fqdn.map</code>
Property aliases	<code>com.sun.identity.agents.config.fqdn.mapping</code> (since 5.0) <code>org.forgerock.agents.fqdn.map</code> (since 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	<code>AgentConfig.properties</code>
AM console tab	<i>Global</i>

Enable FQDN Checking

FQDN Check

When `true`, the FQDN default value and FQDN map value are checked.

Property name	<code>org.forgerock.agents.fqdn.check.enabled</code>
Property aliases	<code>com.sun.identity.agents.config.fqdn.check.enable</code> (since 5.0) <code>org.forgerock.agents.fqdn.check.enabled</code> (since 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	<i>Global</i>

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>
Property aliases	<code>org.forgerock.agents.prometheus.monitoring.enabled</code> (since 5.6)
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	AgentBootstrap.properties
AM console tab	<i>Monitoring</i>

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>
---------------	--

Property aliases	org.forgerock.agents.302.redirect.http.data (since 5.8.0)
Type	String
Default	{ "redirect": { "requestUri": "%REQUEST_URI%", "requestUrl": "%REQUEST_URL%", "targetUrl": "%TARGET%" } }
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	AgentConfig.properties
AM console tab	<i>Miscellaneous</i>

HTTP 302 Redirect Not-Enforced List

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	org.forgerock.agents.config.json.url
Property aliases	org.forgerock.agents.config.json.url (since 5.8.0) org.forgerock.agents.302.redirect.ner.list (since 5.8.0)
Type	List
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	AgentConfig.properties
AM console tab	<i>Miscellaneous</i>

HTTP 302 Redirect Replacement HTTP Status Code

HTTP 302 Redirect Replacement HTTP 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>
Property aliases	<code>org.forgerock.agents.302.redirect.http.status.code</code> (since 5.8.0) <code>org.forgerock.agents.config.json.response.code</code> (since 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	<i>Miscellaneous</i>

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%2Fwww.example.com%3A8020%2Fmanagers%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>
Property aliases	<code>com.sun.identity.agents.config.redirect.param</code> (since 5.0)
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	<i>Miscellaneous</i>

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>
Property aliases	<code>org.forgerock.agents.302.redirect.http.content.type</code> (since 5.8.0)
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	<i>Miscellaneous</i>

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>
Property aliases	<code>org.forgerock.agents.config.json.url.invert</code> (since 5.8.0) <code>org.forgerock.agents.302.redirect.invert.enabled</code> (since 5.8.0)
Type	Boolean: <code>true</code> returns <code>true</code> ; 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	<i>Miscellaneous</i>

Enable HTTP 302 Redirects

HTTP 302 Redirects Enabled

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>
Property aliases	<code>org.forgerock.agents.302.redirects.enabled</code> (since 5.8.0)
Type	Boolean: true returns true; all other strings return false.
Default	true
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>
AM console tab	<i>Miscellaneous</i>

Legacy Support

Enable Legacy Support Handlers (deprecated)

Legacy User Agent Support Enable

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

Property name	<code>org.forgerock.agents.legacy.support.enabled</code>
Deprecated since	5.6

Property aliases	com.sun.identity.agents.config.legacy.support.enabled (since 5.0) org.forgerock.agents.legacy.support.enabled (since 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	<i>Miscellaneous</i>

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	org.forgerock.agents.legacy.redirect.uri
Deprecated since	5.6
Property aliases	com.sun.identity.agents.config.legacy.redirect.uri (since 5.0) org.forgerock.agents.legacy.redirect.uri (since 5.6)
Type	String
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	AgentConfig.properties
AM console tab	<i>Miscellaneous</i>

Legacy User Agent List (deprecated)

A list of legacy user agents.

Property name	<code>org.forgerock.agents.legacy.user.agent.list</code>
Deprecated since	5.6
Property aliases	<code>com.sun.identity.agents.config.legacy.user.agent</code> (since 5.0) <code>org.forgerock.agents.legacy.user.agent.list</code> (since 5.6)
Type	List
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>
AM console tab	<i>Miscellaneous</i>

Locale

Locale Country

The agent country. Changing this has little or not practical effect.

Property name	<code>org.forgerock.agents.locale.country</code>
Property aliases	<code>org.forgerock.agents.locale.country</code> (since 5.6) <code>com.sun.identity.agents.config.locale.country</code> (since 5.0)
Type	String
Default	US
Bootstrap property	No

Required property	No
Restart required	No
Local configuration file	AgentConfig.properties
AM console tab	<i>Miscellaneous</i>

Locale Language

The agent language. Changing this has little or not practical effect.

Property name	org.forgerock.agents.locale.language
Property aliases	org.forgerock.agents.locale.language (since 5.6) com.sun.identity.agents.config.locale.language (since 5.0)
Type	String
Default	en
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	AgentConfig.properties
AM console tab	<i>Miscellaneous</i>

Login

Enable Redirect to AM Success URL

Redirect to AM's 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>
Property aliases	<code>org.forgerock.agents.authn.success.redirect.session.url.enabled</code> (since 5.6.3.0)
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>
AM console tab	<i>AM Services</i>

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 single browser session. After this number, the agent blocks requests from the user.

Property name	<code>org.forgerock.agents.login.attempt.limit.count</code>
Property aliases	<code>org.forgerock.agents.login.attempt.limit.count</code> (since 5.6) <code>com.sun.identity.agents.config.login.attempt.limit</code> (since 5.0)
Type	Integer
Default	<code>0</code>
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>

AM console tab	<i>Global</i>
----------------	---------------

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>
Property aliases	<code>org.forgerock.agents.authn.exchange.cookie.name</code> (since 5.7)
Type	String
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>
AM console tab	SSO

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>
Property aliases	<code>com.sun.identity.agents.config.login.counter.name</code> (since 5.0) <code>org.forgerock.agents.login.counter.cookie.name</code> (since 5.6)
Type	String
Default	<code>amFilterParam</code>
Bootstrap property	No
Required property	No

Restart required	No
Local configuration file	AgentConfig.properties
AM console tab	<i>Global</i>

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>
Property aliases	<code>org.forgerock.agents.login.reason.remapper</code> (since 5.7) <code>org.forgerock.agents.login.reason.map</code> (since 5.7)
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	AgentConfig.properties
AM console tab	<i>Miscellaneous</i>

Redirect Attempt Limit

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

Property name	<code>org.forgerock.agents.redirect.attempt.limit</code>
Property aliases	<code>org.forgerock.agents.redirect.attempt.limit</code> (since 5.6) <code>com.sun.identity.agents.config.redirect.attempt.limit</code> (since 5.0)
Type	Integer
Default	0
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>
AM console tab	<i>Global</i>

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>
Property aliases	<code>org.forgerock.agents.authn.exchange.uri</code> (since 5.7)
Type	String
Bootstrap property	No
Required property	No
Restart required	No

Local configuration file	AgentConfig.properties
AM console tab	SSO

Login URL

OAuth Login URL List

AM Conditional Login URL

Use this property in the default configuration (where Enable Custom Login Mode is `false` and AM Login URL List is empty).

Conditionally redirect unauthenticated requests based on the requested URL.

If the incoming request URL matches a domain name in this list, the agent redirects the unauthenticated request to the specified URL for login. The URL can be an AM instance, site, or a different website.

If Enable FQDN Checking is `true`, the agent iterates through the list of URLs until it finds an appropriate redirect URL that matches the FQDN check values. Otherwise, the agent redirects the user to the URL configured in the conditional redirect rules.

During the redirect, the agent appends the `goto` parameter configured in Goto Parameter Name, and a nonce parameter, to the agent's CDSSO endpoint.

Format, with no spaces between values:

```
[Domain/path] | [URL?realm=value&parameter1=value1...]
```

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 redirection 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
```

?realm=value

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
```

You do not need to specify the realm in the login URL if any of the following conditions is 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.

¶meter1=value1

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

Examples

```
org.forgerock.openam.agents.config.conditional.login.url[0]=  
thisdomain.com|?realm=blue
```

```
org.forgerock.openam.agents.config.conditional.login.url[1]=  
thatdomain.net|?realm=red
```

```
org.forgerock.openam.agents.config.conditional.login.url[2]=  
thatdomain.net/that/path|?realm=grey
```

Property name	org.forgerock.agents.oauth.login.url.list
Property aliases	org.forgerock.agents.oauth.login.url.list (since 5.6) org.forgerock.openam.agents.config.conditional.login.url (since 5.6)
Type	List
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	AgentConfig.properties
AM console tab	<i>AM Services</i>

Enable Custom Login Mode

Allow Custom Login Mode

Set the login redirection mode, as follows:

- `false`: Use the default login redirection mode. This mode uses OpenID Connect ID tokens (JWTs) for authentication. Use with [OAuth Login URL List](#) to modify or redirect calls to the endpoint which provides the tokens.
- `true`: Use the custom login redirection mode, for more control on where the agent redirects the user for authentication. Use with [AM Login URL List](#) and [Legacy Login URL List](#) to modify or redirect calls 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
Property aliases	org.forgerock.agents.legacy.login.enabled (since 5.6) org.forgerock.openam.agents.config.allow.custom.login (since 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	<i>AM Services</i>

Conditional Logout URL List

AM Conditional Logout URL

Allows additional parameters to be conditionally added to legacy logout URLs, using this format:

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

Property name	org.forgerock.agents.conditional.logout.url.list
Property aliases	org.forgerock.openam.agents.config.conditional.logout.url (since 5.6) org.forgerock.agents.conditional.logout.url.list (since 5.6)

Type	List
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	AgentConfig.properties
AM console tab	AM Services

AM Login URL List

AM Login URL

The URL of a custom login page to which the agent redirects users for authentication.

During the redirect, the agent appends the goto parameter configured in [Goto Parameter Name](#), and a nonce parameter, to the agent's CDSSO endpoint.

Format

URL[?realm=realm_name?parameter1=value1&...]

URL

Custom login page to which the agent redirects an unauthenticated user.

[?realm=realm_name¶meter1=value1&...]

Optional parameters that the agent passes to the custom login page, for example, the AM realm where the user is authenticated. You do not need to specify the 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. In this case, ensure the custom login page always returns a realm parameter to the agent.
- The realm into which the agent logs the user 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 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>
Property aliases	<code>com.sun.identity.agents.config.login.url</code> (since 5.0)
Type	List
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>
AM console tab	<i>AM Services</i>

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
Property aliases	org.forgerock.agents.login.reason.parameter.name (since 5.7)
Type	String
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	AgentConfig.properties
AM console tab	<i>Miscellaneous</i>

Legacy Login URL List

Custom Conditional Login URL

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>
---------------	---

Property aliases	org.forgerock.openam.agents.config.conditional.custom.login.url (since 5.6) org.forgerock.agents.legacy.login.url.list (since 5.6)
Type	List
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	AgentConfig.properties
AM console tab	<i>AM Services</i>

Logout

Logout URI Map

Application Logout URI

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

web application name:logout URI

To set a global logout URI for web applications without other logout URIs defined, leave the key empty, and set the value as `/logout.jsp`.

To set a logout URI for a specific web application, set the key to the name of the web application, and set the value to the value of web application logout page.

Property name	org.forgerock.agents.logout.endpoint.map
Property aliases	com.sun.identity.agents.config.logout.uri (since 5.0) org.forgerock.agents.logout.endpoint.map (since 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	AgentConfig.properties
AM console tab	<i>Application</i>

Logout Request Parameter Map

Logout Request Parameter

Map of parameters in the HTTP request that trigger logout events. Use the following key:value format:

web application name:parameter name to trigger logout

To set a global logout request parameter for web applications without other logout request parameters defined, leave the key empty, and set the value to `logoutparam`.

To set a logout URI for a specific web application, set the key to the name of the web application, and set the value to an web application logout request parameter, such as `logoutparam`.

Property name	<code>org.forgerock.agents.logout.request.param.map</code>
Property aliases	<code>org.forgerock.agents.logout.request.param.map</code> (since 5.6) <code>com.sun.identity.agents.config.logout.request.param</code> (since 5.0)
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	AgentConfig.properties
AM console tab	<i>Application</i>

Enable Logout Introspection

Logout Introspect Enabled

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>
Property aliases	<code>com.sun.identity.agents.config.logout.introspect.enabled</code> (since 5.0) <code>org.forgerock.agents.logout.introspection.enabled</code> (since 5.6)
Type	Boolean: <code>true</code> returns <code>true</code> ; 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	<i>Application</i>

Logout Entry URI Map

Logout Entry URI

A map of request URIs to go to after logout using an endpoint defined in [Logout URI Map](#).

To set a global URI for web applications without other logout URIs defined, leave the key empty, and set a return URI such as `/return.html`.

To set a logout URI for a specific web application, set the key to the name of the web application, and set the return URI to the value of web application logout entry URI, such as `/myApp/return.html`.

Property name	<code>org.forgerock.agents.logout.goto.map</code>
Property aliases	<code>com.sun.identity.agents.config.logout.entry.uri</code> (since 5.0) <code>org.forgerock.agents.logout.goto.map</code> (since 5.6)
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	<code>AgentConfig.properties</code>
AM console tab	<i>Application</i>

Logs

Log File Directory

The full path to the directory where the agent writes debug log files after startup.

During agent startup, the location of the logs is based on the container which is being used. For example, bootstrap logs for Tomcat agents are written to `catalina.out`.

The default is set by the installer and written to the bootstrap properties file.

Default: `/logs/debug` directory relative to the location of the agent installation

Property name	<code>com.ipplanet.services.debug.directory</code>
Property aliases	<code>com.ipplanet.services.debug.directory</code> (since 5.0)
Type	String
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>

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>
Property aliases	<code>org.forgerock.agents.redirect.cookie.name</code> (since 5.6) <code>com.sun.identity.agents.config.redirect.cookie.name</code> (since 5.0)
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	<i>Global</i>

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](#).

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>
Property aliases	<code>com.iplanet.am.service.secret</code> (since 5.0) <code>org.forgerock.agents.encrypted.password</code> (since 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

Ignore Path Info for Not Enforced URLs

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>
Property aliases	<code>com.sun.identity.agents.config.ignore.path.info</code> (since 5.0) <code>org.forgerock.agents.ignore.path.info.enabled</code> (since 5.6)
Type	Boolean: <code>true</code> returns true; all other strings return <code>false</code> .

Default	false
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	AgentConfig.properties
AM console tab	Miscellaneous

Custom Response Header Map

Custom Response Header

Format `org.forgerock.agents.response.header.map[HEADER_NAME]=HEADER_VALUE`

Custom headers the agent sets for the client. The key is the header name. The value is the header value. For example, `org.forgerock.agents.response.header.map[Cache-Control]=no-cache`

Property name	<code>org.forgerock.agents.response.header.map</code>
Property aliases	<code>org.forgerock.agents.response.header.map</code> (since 5.6) <code>com.sun.identity.agents.config.response.header</code> (since 5.0)
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	AgentConfig.properties
AM console tab	Global

Idle Time Refresh Window

The time in minutes the agent waits before calling AM to refresh a the 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>
Property aliases	<code>org.forgerock.agents.idle.time.window.minutes</code> (since 5.6.2.1)
Type	Integer
Default	1
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>
AM console tab	<i>Advanced</i>

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>
Property aliases	<code>org.forgerock.agents.service.resolver.class.name</code> (since 5.6.2.1)
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>
Property aliases	<code>com.sun.identity.agents.config.httpsession.binding</code> (since 5.0) <code>org.forgerock.agents.http.session.binding.enabled</code> (since 5.6)
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	AgentConfig.properties
AM console tab	Global

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
Property aliases	com.forgerock.agents.public.am.url (since 5.6.3.0) org.forgerock.agents.public.am.url (since 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>
Property aliases	<code>org.forgerock.agents.config.monitoring.to.csv</code> (since 5.6) <code>org.forgerock.agents.monitoring.to.csv.enabled</code> (since 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	<i>Advanced</i>

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 location of the agent installation

Property name	<code>org.forgerock.agents.csv.monitoring.directory</code>
---------------	--

Property aliases	<code>org.forgerock.agents.csv.monitoring.directory</code> (since 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

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>
Property aliases	<code>org.forgerock.agents.not.enforced.rule.pattern.matcher.classname</code> (since 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

Enable Not-Enforced IP Cache

NOTE

The use of this property is NOT recommended.

Not Enforced IP Cache Flag

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>
Property aliases	<code>org.forgerock.agents.notenforced.ip.cache.enabled</code> (since 5.6) <code>com.sun.identity.agents.config.notenforced.ip.cache.enabled</code> (since 5.0)
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	<i>Application</i>

Not-Enforced URIs

Not Enforced URIs

A space-delimited list of URIs that do not require authentication. See the documentation for details.

Property name	<code>org.forgerock.agents.notenforced.uri.list</code>
---------------	--

Property aliases	org.forgerock.agents.notenforced.uri.list (since 5.6) com.sun.identity.agents.config.notenforced.uri (since 5.0)
Type	List
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	AgentConfig.properties

Invert Not-Enforced IPs

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	org.forgerock.agents.notenforced.ip.invert.enabled
Property aliases	org.forgerock.agents.notenforced.ip.invert.enabled (since 5.6) com.sun.identity.agents.config.notenforced.ip.invert (since 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	<i>Application</i>

Not-Enforced Client IP List

Not Enforced Client IP List

A space-delimited list of IP addresses or network CIDR notation addresses for which no authentication is required.

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	org.forgerock.agents.notenforced.ip.list
Property aliases	org.forgerock.agents.notenforced.ip.list (since 5.6) com.sun.identity.agents.config.notenforced.ip (since 5.0)
Type	List
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	AgentConfig.properties

Not-Enforced Favicon

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	org.forgerock.agents.auto.not.enforce.favicon
---------------	---

Property aliases	org.forgerock.agents.auto.not.enforce.favicon (since 5.7) org.forgerock.agents.auto.not.enforce.favicon.enabled (since 5.7)
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	AgentBootstrap.properties
AM console tab	<i>Application</i>

Enable Not-Enforced URIs Cache

Not Enforced URIs Cache Enabled

When `true`, the agent caches evaluations of the Not-Enforced URIs.

Enable this setting when configuring many rules.

Property name	org.forgerock.agents.notenforced.uri.cache.enabled
Property aliases	org.forgerock.agents.notenforced.uri.cache.enabled (since 5.6) com.sun.identity.agents.config.notenforced.uri.cache.enable (since 5.0)
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	<i>Application</i>

Max Entries in Not-Enforced IP Cache

Not Enforced IP Cache Size

The maximum number of cached IP addresses that are matched by a not-enforced rule (inverted or not inverted).

Property name	org.forgerock.agents.notenforced.ip.cache.size
Property aliases	org.forgerock.agents.notenforced.ip.cache.size (since 5.6) com.sun.identity.agents.config.notenforced.ip.cache.size (since 5.0)
Type	Integer
Default	1000
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	AgentConfig.properties
AM console tab	<i>Application</i>

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>
Property aliases	<code>org.forgerock.agents.notenforced.compound.separator</code> (since 5.6) <code>com.sun.identity.agents.config.notenforced.rule.compound.separator</code> (since 5.0)
Type	String
Default	
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>
AM console tab	<i>Application</i>

Invert Not-Enforced URIs

NOTE

The use of this property is NOT recommended.

Invert Not Enforced URIs

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>
Property aliases	<code>com.sun.identity.agents.config.notenforced.uri.invert</code> (since 5.0) <code>org.forgerock.agents.notenforced.uri.invert.enabled</code> (since 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	<i>Application</i>

Max Entries in Not-Enforced URI Cache

Not Enforced URIs Cache Size

The maximum number of cached resource URLs that are matched by a not-enforced rule (inverted or not inverted).

Property name	org.forgerock.agents.notenforced.uri.cache.size
Property aliases	com.sun.identity.agents.config.notenforced.uri.cache.size (since 5.0) org.forgerock.agents.notenforced.uri.cache.size (since 5.6)
Type	Integer
Default	10000
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	AgentConfig.properties
AM console tab	<i>Application</i>

Notifications

Enable Notifications of Agent Configuration Change

Agent Configuration Change Notification

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>
Property aliases	<code>org.forgerock.agents.config.change.notifications.enabled</code> (since 5.6) <code>com.sun.identity.agents.config.change.notification.enable</code> (since 5.0)
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	No
Local configuration file	<code>AgentBootstrap.properties</code>
AM console tab	<i>Global</i>

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 since	5.6

Property aliases	<code>com.sun.identity.client.notification.url</code> (since 5.0) <code>org.forgerock.agents.obsolete.notification.url</code> (since 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)

Flag to indicate whether the agent subscribes to WebSocket notifications from AM for session logout.

Use [Enable Notification of Session Logout](#) instead of this property.

Property name	<code>com.ipplanet.am.session.client.polling.enabled</code>
Deprecated since	5.6
Property aliases	<code>com.ipplanet.am.session.client.polling.enabled</code> (since 5.6) <code>com.ipplanet.am.session.client.polling.enable</code> (since 5.0)
Type	Boolean: <code>true</code> returns true; all other strings return <code>false</code> .
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>

Enable Notification of Policy Changes

Flag to indicate whether the agent subscribes to WebSocket notifications from AM for policy changes.

Property name	<code>org.forgerock.agents.policy.change.notifications.enabled</code>
Property aliases	<code>org.forgerock.agents.policy.change.notifications.enabled</code> (since 5.6) <code>com.sun.identity.agents.notification.enabled</code> (since 5.0)
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	No
Local configuration file	<code>AgentBootstrap.properties</code>
AM console tab	<i>AM Services</i>

Enable Notification of Session Logout

Flag to indicate whether the agent subscribes to WebSocket notifications from AM for session logout.

If this property and [Enable Notification of Session Logout \(deprecated\)](#) are not set, the agent subscribes to WebSocket notifications from AM for session logout.

Property name	<code>org.forgerock.agents.session.change.notifications.enabled</code>
Property aliases	<code>org.forgerock.agents.session.change.notifications.enabled</code> (since 5.6)
Type	Boolean: <code>true</code> returns true; all other strings return <code>false</code> .

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

POST Data Preservation

POST Data Preservation Sticky Session Mode

PDP Stickysession mode

Property name	org.forgerock.agents.pdp.sticky.session.mode
Property aliases	org.forgerock.agents.pdp.sticky.session.mode (since 5.6) com.sun.identity.agents.config.postdata.preserve.stickysession.mode (since 5.0)
Supported settings	COOKIE 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)). URL 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)).
Default	URL
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	AgentConfig.properties
AM console tab	<i>Advanced</i>

Enable POST Data Preservation

Post Data Preservation enabled

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>
Property aliases	<code>org.forgerock.agents.post.data.preservation.enabled</code> (since 5.6) <code>com.sun.identity.agents.config.postdata.preserve.enable</code> (since 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	<code>AgentConfig.properties</code>
AM console tab	<i>Advanced</i>

Missing POST Data Preservation Entry URI Map

Missing PDP entry URI

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>
---------------	---

Property aliases	org.forgerock.agents.pdp.noentry.url.map (since 5.6) com.sun.identity.agents.config.postdata.preserve.cache.noentry.url (since 5.0)
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	AgentConfig.properties
AM console tab	<i>Advanced</i>

POST Data Preservation Cache Size

PDP Maximum Cache Size

The maximum number of megabytes allocated to the POST data preservation cache. When the cache reaches the maximum, 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 Cache](#).

Property name	org.forgerock.agents.pdp.cache.total.size.mb
Property aliases	org.forgerock.agents.pdp.cache.total.size.mb (since 5.6) org.forgerock.openam.agents.config.postdata.preserve.cache.entry.max.total.size.mb (since 5.6)
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 tab	<i>Advanced</i>

Max Entries in POST Data Preservation Cache

PDP Maximum Number of Cache Entries

The maximum number of entries in the POST data preservation cache. When the cache reaches the maximum, old entries are discarded.

Use this property to mitigate the risk of DoS attacks.

POST Data Preservation Cache Size takes precedence over this property.

Property name	org.forgerock.agents.pdp.cache.size
Property aliases	org.forgerock.agents.pdp.cache.size (since 5.6) org.forgerock.openam.agents.config.postdata.preserve.cache.entry.max.entries (since 5.6)
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	<i>Advanced</i>

POST Data Preservation Cache TTL

PDP Cache TTL in Minutes

The time in minutes after 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>
Property aliases	<code>org.forgerock.agents.pdp.cache.ttl.minutes</code> (since 5.6)
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	<i>Advanced</i>

POST Data Preservation Sticky Session Key Value

PDP Stickysession 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>
Property aliases	<code>com.sun.identity.agents.config.postdata.preserve.stickysession.value</code> (since 5.0) <code>org.forgerock.agents.pdp.sticky.session.value</code> (since 5.6)
Type	String

Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	AgentConfig.properties
AM console tab	<i>Advanced</i>

POST Data Preservation Cache TTL in Milliseconds (deprecated)

PDP Cache TTL in Milliseconds

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 since	5.6
Property aliases	
Type	Integer
Default	''
Bootstrap property	Yes
Required property	No
Restart required	Yes - Restart the container after changing the property
Local configuration file	AgentBootstrap.properties

Policy Client Service

Session Cache TTL

The time in minutes after 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>
Property aliases	<code>org.forgerock.agents.session.cache.ttl.minutes</code> (since 5.6) <code>org.forgerock.openam.agents.config.active.session.cache.ttl.minutes</code> (since 5.0)
Type	Integer
Default	15
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	<i>Advanced</i>

POST Parameter List for URL Policy Env

URL Policy Env POST Parameters

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>
Property aliases	<code>com.sun.identity.agents.config.policy.env.post.param</code> (since 5.0) <code>org.forgerock.agents.continuous.security.post.list</code> (since 5.7)
Type	List
Bootstrap property	No

Required property	No
Restart required	No
Local configuration file	AgentConfig.properties
AM console tab	AM Services

Max Entries in Policy Cache per Session

Policy Cache Per User

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	org.forgerock.agents.policy.cache.per.session.size
Property aliases	com.sun.identity.policy.client.cacheResultsPerUserCap (since 5.0) org.forgerock.agents.policy.cache.per.session.size (since 5.6)
Type	Integer
Default	50
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

Restrict to Realm Map

Restrict To Realm

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>
Property aliases	<code>org.forgerock.agents.restrict.to.realm.map</code> (since 5.6.2.1)
Type	Map <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	<code>AgentConfig.properties</code>
AM console tab	<i>AM Services</i>

Enable Composite Advice Encoding

Composite Advice Encode

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>
Property aliases	<code>com.forgerock.agents.advice.b64.url.encode</code> (since 5.6.2.1) <code>org.forgerock.agents.advice.b64.url.encode.enabled</code> (since 5.6.2.1) <code>org.forgerock.agents.advice.b64.url.encode</code> (since 5.6.2.1)
Type	Boolean: <code>true</code> returns true; all other strings return <code>false</code> .

Default	false
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	AgentConfig.properties
AM console tab	AM Services

Max Sessions in Policy Cache

Policy Cache Size

The maximum number of sessions (distinct users) that can be stored in the policy evaluation cache at any time.

Property name	org.forgerock.agents.policy.cache.session.size
Property aliases	org.forgerock.agents.policy.cache.session.size (since 5.6) com.sun.identity.policy.client.cachedSessionCap (since 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	AgentBootstrap.properties
AM console tab	Advanced

Enable Policy Evaluation in User Authentication Realm

Perform Policy Evaluation in User Authenticated 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>
Property aliases	<code>org.forgerock.agents.user.realm.overrides.policy.evaluation.realm.enabled</code> (since 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	<i>AM Services</i>

GET Parameter List for URL Policy Env

URL Policy Env GET Parameters

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>
Property aliases	<code>com.sun.identity.agents.config.policy.env.get.param</code> (since 5.0) <code>org.forgerock.agents.continuous.security.get.list</code> (since 5.7)
Type	List
Bootstrap property	No

Required property	No
Restart required	No
Local configuration file	AgentConfig.properties
AM console tab	AM Services

Policy Cache TTL

The time in minutes after which entries in the policy cache time out and are purged.

Property name	org.forgerock.agents.policy.cache.ttl.minutes
Property aliases	org.forgerock.agents.policy.cache.ttl.minutes (since 5.6) com.sun.identity.agents.polling.interval (since 5.0)
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

JSession Parameter List for URL Policy Env

URL Policy Env jsession Parameters

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	org.forgerock.agents.continuous.security.http.session.list
---------------	--

Property aliases	org.forgerock.agents.continuous.security.http.session.list (since 5.7) com.sun.identity.agents.config.policy.env.jsession.param (since 5.0)
Type	List
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	AgentConfig.properties
AM console tab	<i>AM Services</i>

Policy Evaluation Realm Map

Policy Evaluation Realm

The realm in which policy evaluation is carried out for a particular request. Different web applications can use different policy realms.

Property name	org.forgerock.agents.policy.evaluation.realm.map
Property aliases	org.forgerock.openam.agents.config.policy.evaluation.realm (since 5.0) org.forgerock.agents.policy.evaluation.realm.map (since 5.6.2.1)
Type	Map <ul style="list-style-type: none"> • Keys: web application • Values: realm
Default	/
Bootstrap property	No
Required property	No
Restart required	No

Local configuration file	AgentConfig.properties
AM console tab	AM Services

Policy Set Map

Policy Set

The policy set in which to evaluate policy requests. Different web applications can use a different policy set in their chosen realm.

The following example causes AM to look in `mypolicyset` to evaluate policies for all web applications:

```
org.forgerock.agents.policy.set.map=mypolicyset
```

The following example causes AM to look in `mypolicyset` to evaluate policies for `mywebapp`. For all other web applications, AM looks in `iPlanetAMWebAgentService`:

```
org.forgerock.agents.policy.set.map[mywebapp]=mypolicyset
```

Property name	<code>org.forgerock.agents.policy.set.map</code>
Property aliases	<code>org.forgerock.openam.agents.config.policy.evaluation.application</code> (since 5.0) <code>org.forgerock.agents.policy.set.map</code> (since 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	AgentConfig.properties
AM console tab	AM Services

Port Check

Port Check Filename (deprecated)

Port Check File

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 since	5.6
Property aliases	<code>com.sun.identity.agents.config.port.check.file</code> (since 5.0) <code>org.forgerock.agents.port.check.file</code> (since 5.6)
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 tab	<i>Miscellaneous</i>

Port Check Protocol Map (deprecated)

Port Check Setting

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 since	5.6

Property aliases	com.sun.identity.agents.config.port.check.setting (since 5.0) org.forgerock.agents.port.check.map (since 5.6)
Type	Map <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	<i>Miscellaneous</i>

Enable Port Checking (deprecated)

Port Check Enable

A flag to enable port checking when the filter mode is `SSO_ONLY`. See [Agent Filter Mode Map](#).

Property name	org.forgerock.agents.port.check.enabled
Deprecated since	5.6
Property aliases	com.sun.identity.agents.config.port.check.enable (since 5.0) org.forgerock.agents.port.check.enabled (since 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	<i>Miscellaneous</i>

Profile

Fall-Forward Mode (deprecated)

Use [Strategy when AM unavailable](#) instead of this property.

Property name	org.forgerock.agents.fallforward.mode.enabled
Deprecated since	5.9
Property aliases	org.forgerock.agents.fallforward.mode.enabled (since 5.7)
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	<i>Global</i>

Location of Agent Configuration Repository

The location of the agent configuration.

Property name	org.forgerock.agents.config.location
Property aliases	com.sun.identity.agents.config.repository.location (since 5.0) org.forgerock.agents.config.location (since 5.6)

Supported settings	<p>LOCAL</p> <p>The agent configuration is read from AgentConfiguration.properties (only).</p> <p>REMOTE</p> <p>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 tab	Global

JWT Cookie Domain List

CDSSO 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	org.forgerock.agents.jwt.cookie.domain.list
Property aliases	<p>com.sun.identity.agents.config.cdsso.domain (since 5.0)</p> <p>org.forgerock.agents.jwt.cookie.domain.list (since 5.6)</p>
Type	List
Bootstrap property	No
Required property	No

Restart required	No
Local configuration file	AgentConfig.properties
AM console tab	SSO

JWT Cache TTL

The time in minutes after which entries in the JWT cache timeout and are purged.

Parsing JWTs is a CPU intensive process. Because all JWTs in the cache have already been parsed, consider using a long timeout for this cache.

Property name	org.forgerock.agents.jwt.cache.ttl.minutes
Property aliases	org.forgerock.openam.agents.config.jwt.cache.ttl.minutes (since 5.0) org.forgerock.agents.jwt.cache.ttl.minutes (since 5.6)
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	<i>Advanced</i>

Max Entries in JWT Cache

JWT Cache Size

The maximum number of entries in the JWT cache.

Property name	org.forgerock.agents.jwt.cache.size
---------------	-------------------------------------

Property aliases	org.forgerock.agents.jwt.cache.size (since 5.6) org.forgerock.openam.agents.config.jwt.cache.size (since 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	AgentBootstrap.properties
AM console tab	<i>Advanced</i>

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.

Property name	org.forgerock.agents.jwt.cookie.name
Property aliases	org.forgerock.openam.agents.config.jwt.name (since 5.0) org.forgerock.agents.jwt.cookie.name (since 5.6)
Type	String
Default	am-auth-jwt
Bootstrap property	Yes
Required property	No
Restart required	No

Local configuration file	AgentBootstrap.properties
AM console tab	Global

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>
Property aliases	<code>org.forgerock.agents.agent.profile.realm</code> (since 5.6) <code>com.sun.identity.agents.config.organization.name</code> (since 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

Exchanged SSO Token Cache Time to Live

The time in minutes after 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	<code>org.forgerock.agents.sso.exchange.cache.ttl.minutes</code>
Property aliases	<code>org.forgerock.agents.sso.exchange.cache.ttl.minutes</code> (since 5.6.2.1)
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	<i>Advanced</i>

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	<code>org.forgerock.agents.config.reload.seconds</code>
Property aliases	<code>com.sun.identity.agents.config.load.interval</code> (since 5.0) <code>org.forgerock.agents.config.reload.seconds</code> (since 5.6)
Type	Integer
Default	0
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>

AM console tab	<i>Global</i>
----------------	---------------

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>
Property aliases	<code>com.sun.identity.agents.app.username</code> (since 5.0) <code>com.sun.identity.agents.config.profilename</code> (since 5.0) <code>org.forgerock.agents.profile.name</code> (since 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>
Property aliases	<code>com.sun.identity.agents.config.lock.enable</code> (since 5.0) <code>org.forgerock.agents.lock.config.enabled</code> (since 5.6)
Type	Boolean: <code>true</code> returns true; all other strings return <code>false</code> .

Default	false
Bootstrap property	Yes
Required property	No
Restart required	No
Local configuration file	AgentBootstrap.properties

Profile Attribute Map

Profile Attribute Mapping

Maps a profile attribute to one or more HTTP headers for the currently authenticated user. The map key is an attribute name, and the map values are HTTP header names. Separate multiple map values with a pipe (|) character.

The user profile can be stored in LDAP or any other arbitrary data store.

To populate the value of profile attribute CN under CUSTOM-Common-Name, enter CN in the Map Key field, and enter CUSTOM-Common-Name in the Corresponding Map Value field. This corresponds to `org.forgerock.agents.profile.attribute.map[cn]=CUSTOM-Common-Name`.

In most cases, in a destination web application where an HTTP header name shows up as a request header, it is prefixed by HTTP_, lower case letters become upper case, and hyphens (-) become underscores (_). For example, `common-name` becomes `HTTP_COMMON_NAME`.

Format: `profile attribute = HEADER_NAME(S)`

Example: `[cn]=HEADER1|HEADER2`

Property name	<code>org.forgerock.agents.profile.attribute.map</code>
Property aliases	<code>com.sun.identity.agents.config.profile.attribute.mapping</code> (since 5.0) <code>org.forgerock.agents.profile.attribute.map</code> (since 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	<i>Application</i>

Max Entries in SSO Exchange Cache

Exchanged SSO Token Cache Size

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>
Property aliases	<code>org.forgerock.agents.sso.exchange.cache.size</code> (since 5.6.2.1)
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	<i>Advanced</i>

Profile Attribute Fetch Mode

The location from where profile attributes are fetched.

Property name	<code>org.forgerock.agents.profile.attribute.fetch.mode</code>
Property aliases	<code>com.sun.identity.agents.config.profile.attribute.fetch.mode</code> (since 5.0) <code>org.forgerock.agents.profile.attribute.fetch.mode</code> (since 5.6)
Supported settings	<i>NONE</i> Attributes are not fetched. <i>HTTP_HEADER</i> Attributes are fetched from HTTP headers. <i>REQUEST_ATTRIBUTE</i> Attributes are fetched from request attributes. <i>HTTP_COOKIE</i> Attributes are fetched from HTTP cookies.
Default	NONE
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>
AM console tab	<i>Application</i>

WebSocket Connection Interval

The time in minutes before 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>
---------------	--

Property aliases	org.forgerock.openam.agents.config.balance.websocket.connection.interval.in.minutes (since 5.6) org.forgerock.agents.balance.websocket.interval.minutes (since 5.6)
Type	Integer
Default	30
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	AgentConfig.properties
AM console tab	<i>Global</i>

Query Parameter Handling

Regex Remove Query Parameters List for Policy Evaluation

Regular Expression Remove Query Parameters

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>
Property aliases	<code>org.forgerock.agents.unwanted.http.url.params.regex.list</code> (since 5.6) <code>org.forgerock.openam.agents.config.conditional.unwanted.http.url.params.regex</code> (since 5.6) <code>org.forgerock.agents.unwanted.http.url.params.regex.list</code> (since 5.6)
Type	List
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>
AM console tab	<i>Miscellaneous</i>

Remove Query Parameters List for Policy Evaluation

Remove Query Parameters

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	org.forgerock.agents.unwanted.http.url.param.list
Property aliases	org.forgerock.agents.unwanted.http.url.param.list (since 5.6) org.forgerock.openam.agents.config.conditional.unwanted.http.url.params (since 5.6)
Type	List
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	AgentConfig.properties

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	<code>org.forgerock.agents.wanted.http.url.params.regexp.list</code>
Property aliases	<code>org.forgerock.agents.wanted.http.url.params.regexp.list</code> (since 5.6) <code>org.forgerock.openam.agents.config.conditional.wanted.http.url.params.regexp</code> (since 5.6) <code>org.forgerock.agents.wanted.http.url.params.regexp.list</code> (since 5.6)
Type	List
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>
AM console tab	<i>Miscellaneous</i>

Query Parameter List for Policy Evaluation

Retain Query Parameters

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>
Property aliases	<code>org.forgerock.openam.agents.config.conditional.wanted.http.url.params</code> (since 5.6) <code>org.forgerock.agents.wanted.http.url.param.list</code> (since 5.6)
Type	List
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>
AM console tab	<i>Miscellaneous</i>

Required

AM Authentication Service Path

The path to the AM server.

Property name	<code>org.forgerock.agents.am.path</code>
Property aliases	<code>com.ipplanet.am.services.deploymentDescriptor</code> (since 5.0) <code>org.forgerock.agents.am.path</code> (since 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>
Property aliases	<code>org.forgerock.agents.am.protocol</code> (since 5.6) <code>com.ipplanet.am.server.protocol</code> (since 5.0)
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>
AM console tab	<i>AM Services</i>

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](#).

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>
Property aliases	<code>com.ipplanet.am.service.secret</code> (since 5.0) <code>org.forgerock.agents.encrypted.password</code> (since 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>
Property aliases	<code>com.sun.identity.agents.config.repository.location</code> (since 5.0) <code>org.forgerock.agents.config.location</code> (since 5.6)

Supported settings	<p>LOCAL</p> <p>The agent configuration is read from AgentConfiguration.properties (only).</p> <p>REMOTE</p> <p>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 tab	Global

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
Property aliases	com.forgerock.agents.public.am.url (since 5.6.3.0) org.forgerock.agents.public.am.url (since 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

Authentication Redirect URI

CDSSO 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>
Property aliases	<code>org.forgerock.agents.authn.redirect.uri</code> (since 5.6) <code>com.sun.identity.agents.config.cdsso.redirect.uri</code> (since 5.0)
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	SSO

Encrypting Java class

The Java class used to encrypt the agent password.

During installation, the class is set in the bootstrap properties file with the default value. Change the class only to reduce your level of encryption.

To change the class, make sure that the class is available at runtime, regenerate the agent password using the agent installer, and manually edit the newly generated encrypted password into the bootstrap properties file.

Property name	<code>org.forgerock.agents.encryptor.classname</code>
Property aliases	<code>org.forgerock.agents.encryptor.classname</code> (since 5.7) <code>com.ipplanet.security.encryptor</code> (since 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	Yes - Restart the container after changing the property
Local configuration file	<code>AgentBootstrap.properties</code>

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>
Property aliases	<code>org.forgerock.agents.agent.profile.realm</code> (since 5.6) <code>com.sun.identity.agents.config.organization.name</code> (since 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

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>
Property aliases	<code>com.sun.identity.agents.app.username</code> (since 5.0) <code>com.sun.identity.agents.config.profilename</code> (since 5.0) <code>org.forgerock.agents.profile.name</code> (since 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	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>
---------------	---

Property aliases	<p><code>com.forgerock.agents.config.fallback.mode</code> (since 5.9.0)</p> <p><code>org.forgerock.agents.fallback.mode.enabled</code> (since 5.9.0)</p> <p><code>org.forgerock.agents.autonomous.mode.enabled</code> (since 5.9.0)</p>
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>

AM Authentication Service Host Name

The AM server host name.

Property name	<code>org.forgerock.agents.am.hostname</code>
Property aliases	<p><code>com.ipplanet.am.server.host</code> (since 5.0)</p> <p><code>org.forgerock.agents.am.hostname</code> (since 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	<code>AgentBootstrap.properties</code>
AM console tab	<i>AM Services</i>

AM Authentication Service Port

The AM server port number.

Property name	<code>org.forgerock.agents.am.port</code>
Property aliases	<code>com.ipplanet.am.server.port</code> (since 5.0) <code>org.forgerock.agents.am.port</code> (since 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	<i>AM Services</i>

Encryption Key

The key with which to encrypt the agent password.

The key is set during installation process. To change it after installation:

- Manually invoke `agentadmin` with the `--getEncryptKey` option
- Manually edit the result into the bootstrap property file, against the encryption key property
- Re-encrypt your password using `agentadmin` with the `--encrypt` option
- Manually edit the encrypted result into the bootstrap property file, against the encrypted password property

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

Property name	<code>am.encryption.pwd</code>
Property aliases	<code>am.encryption.pwd</code> (since 5.0)
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	AgentKey.properties
--------------------------	---------------------

Response

Response Attribute Map

Response Attribute Mapping

Maps a policy response attribute to one or more HTTP headers for the currently authenticated user. The map key is an attribute name, and the map values are HTTP header names. Separate multiple map values with a pipe (|) character.

The response attribute is the attribute in the policy response to be fetched.

To populate the value of response attribute `uid` under `CUSTOM-User-Name`, enter `uid` in the `Map Key` field, and enter `CUSTOM-User-Name` in the `Corresponding Map Value` field. This corresponds to `org.forgerock.agents.response.attribute.map[uid]=Custom-User-Name`.

In most cases, in a destination web application where an HTTP header name shows up as a request header, it is prefixed by `HTTP_`; lower case letters become upper case, and hyphens (-) become underscores (_). For example, `response-attr-one` becomes `HTTP_RESPONSE_ATTR_ONE`.

Format: `response attribute = HEADER_NAME(S)`

Example: `[uid]=HEADER1|HEADER2`

Property name	<code>org.forgerock.agents.response.attribute.map</code>
Property aliases	<code>org.forgerock.agents.response.attribute.map</code> (since 5.6) <code>com.sun.identity.agents.config.response.attribute.mapping</code> (since 5.0)
Type	Map <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	AgentConfig.properties
AM console tab	<i>Application</i>

Response Attribute Fetch Mode

The location from where response attributes are fetched.

Property name	org.forgerock.agents.response.attribute.fetch.mode
Property aliases	com.sun.identity.agents.config.response.attribute.fetch.mode (since 5.0) org.forgerock.agents.response.attribute.fetch.mode (since 5.6)
Supported settings	NONE Attributes are not fetched. HTTP_HEADER Attributes are fetched from HTTP headers. REQUEST_ATTRIBUTE Attributes are fetched from request attributes. HTTP_COOKIE Attributes are fetched from HTTP cookies.
Default	NONE
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	AgentConfig.properties
AM console tab	<i>Application</i>

SSO Cookie Handling

Enable SSO Token Acceptance

Accept SSO Tokens

Set this property as follows:

- `true` : Accept SSO tokens. Use this option when the agent and the token issuer are in the same domain.
- `false` : Do not accept SSO tokens. Use this option for web applications and APIs where the backend requires user information in form of an OIDC token.

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>
Property aliases	<code>org.forgerock.agents.accept.sso.tokens.enabled</code> (since 5.7.1) <code>org.forgerock.agents.accept.sso.tokens</code> (since 5.7.1) <code>com.forgerock.agents.accept.sso.tokens</code> (since 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

Convert SSO Tokens Into OIDC JWTs

Convert SSO Tokens into OpenID Connect JWTs

When `true`, the agent makes a request to AM to convert SSO tokens into OIDC JWTs, to make them compliant with the agent default login redirection mode.

Set this property to let users access resources protected with systems that continue to use SSO tokens, as opposed to the more secure OIDC JWTs. Converting SSO tokens to JWTs negates the need for additional redirection or re-authentication.

The client web application is responsible for appending the JWT to subsequent calls to protected resources. Failure to do so causes the agent to request additional JWTs from AM.

Property name	<code>org.forgerock.agents.accept.ipdp.cookie</code>
Property aliases	<code>com.forgerock.agents.accept.ipdp.cookie</code> (since 5.6) <code>org.forgerock.agents.accept.ipdp.cookie.enabled</code> (since 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

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>
Property aliases	<code>org.forgerock.agents.ipdp.cookie.domain.list</code> (since 5.7.1)
Type	List
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>
AM console tab	<i>SSO</i>

Session

Session Attribute Fetch Mode

The location from where session attributes are fetched.

Property name	<code>org.forgerock.agents.session.attribute.fetch.mode</code>
Property aliases	<code>org.forgerock.agents.session.attribute.fetch.mode</code> (since 5.6) <code>com.sun.identity.agents.config.session.attribute.fetch.mode</code> (since 5.0)

Supported settings	<p>NONE Attributes are not fetched.</p> <p>HTTP_HEADER Attributes are fetched from HTTP headers.</p> <p>REQUEST_ATTRIBUTE Attributes are fetched from request attributes.</p> <p>HTTP_COOKIE Attributes are fetched from HTTP cookies.</p>
Default	NONE
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	AgentConfig.properties
AM console tab	Application

Session Attribute Map

Session Attribute Mapping

Maps a session attribute to one or more HTTP headers for the currently authenticated user. The map key is an attribute name, and the map values are HTTP header names. Separate multiple map values with a pipe (|) character.

The session attribute is the attribute in the session to be fetched.

To populate the value of session attribute `UserToken` under `CUSTOM-userid`, enter `UserToken` in the Map Key field, and enter `CUSTOM-userid` in the Corresponding Map Value field. This corresponds to `org.forgerock.agents.session.attribute.map[UserToken]=CUSTOM-userid`.

In most cases, in a destination web application where an HTTP header name shows up as a request header, it is prefixed by `HTTP_`, lower case letters become upper case, and hyphens (-) become underscores (_). For example, `success-ur1` becomes `HTTP_SUCCESS_URL`.

Format: `session attribute = HEADER_NAME(S)`

Example: `[UserToken]=HEADER1|HEADER2`

Property name	<code>org.forgerock.agents.session.attribute.map</code>
Property aliases	<code>org.forgerock.agents.session.attribute.map</code> (since 5.6) <code>com.sun.identity.agents.config.session.attribute.mapping</code> (since 5.0)
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	<code>AgentConfig.properties</code>
AM console tab	<i>Application</i>

Max Entries in Expired Session Cache

Expired Session Cache Max Records

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>
Property aliases	<code>org.forgerock.agents.expired.session.cache.size</code> (since 5.7.1)
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	<i>Advanced</i>
----------------	-----------------

Expired Session Cache Timeout

The time in minutes after 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.timeout.minutes</code>
Property aliases	<code>org.forgerock.agents.sso.expired.session.cache.timeout.minutes</code> (since 5.7.1)
Type	Integer
Default	20
Bootstrap property	Yes
Required property	No
Restart required	Yes - Restart the container after changing the property
Local configuration file	<code>AgentBootstrap.properties</code>
AM console tab	<i>Advanced</i>

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>
---------------	--

Property aliases	<code>org.forgerock.agents.ping.websocket.after.inactive.milliseconds</code> (since 5.8)
Type	Integer
Default	20000
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>

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>
Property aliases	<code>org.forgerock.agents.declare.websocket.dead.after.milliseconds</code> (since 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>
Property aliases	<code>com.sun.identity.agents.config.user.attribute.name</code> (since 5.0) <code>org.forgerock.agents.user.mapping.mode.attribute.name</code> (since 5.6)
Type	String
Default	<code>employeenumber</code>
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>
AM console tab	<i>Global</i>

User Mapping Mode

Specifies where to obtain the user ID

Property name	<code>org.forgerock.agents.user.mapping.mode</code>
Property aliases	<code>org.forgerock.agents.user.mapping.mode</code> (since 5.6) <code>com.sun.identity.agents.config.user.mapping.mode</code> (since 5.0)

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 tab	Global

User Session Name

User Token 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	<code>org.forgerock.agents.userid.mapping.mode.use.session.property.name</code>
Property aliases	<code>com.sun.identity.agents.config.user.token</code> (since 5.0) <code>org.forgerock.agents.userid.mapping.mode.use.session.property.name</code> (since 5.6)
Type	String
Default	UserToken
Bootstrap property	No
Required property	No
Restart required	No
Local configuration file	<code>AgentConfig.properties</code>
AM console tab	<i>Global</i>

Enable User Principal Flag

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	<code>org.forgerock.agents.userid.mapping.mode.use.dn.enabled</code>
Property aliases	<code>com.sun.identity.agents.config.user.principal</code> (since 5.0) <code>org.forgerock.agents.userid.mapping.mode.use.dn.enabled</code> (since 5.6)
Type	Boolean: <code>true</code> returns <code>true</code> ; 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	<i>Global</i>

Copyright © 2010-2023 ForgeRock, all rights reserved.