

# 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 files

The agent stores agent bootstrap and configuration properties in one file, `agent.conf`.

For IIS Web Agent, the file is located by default at

`C:\web_agents\iis_agent\instances\agent_1\config\agent.conf`

## Bootstrap properties

The agent configurations support the following bootstrap properties:

- [Accept Secure Cookies From AM Over HTTP](#)
- [Agent Debug File Size](#)
- [Agent Debug Level](#)
- [Agent Profile Name](#)
- [Agent Profile Password](#)
- [Agent Profile Password Encryption Key](#)
- [Agent Profile Realm](#)
- [AM Connection URL](#)
- [CA Certificate File Name](#)
- [Connection Timeout](#)
- [Enable Connection Pooling](#)
- [Enable Fragment Redirect](#)
- [Enable Multivalue for Pre-Authn Cookie](#)
- [Enable Notifications](#)
- [Enable OpenSSL to Secure Internal Communications](#)
- [Hostname to IP Address Map](#)
- [JWT Cookie Name](#)

- Local Agent Audit File Name
- Local Agent Debug File Name
- Local Audit Log Rotation Size
- Location of Agent Configuration Repository
- Maximum Number of Debug Log Files
- Not-Enforced Fallback Mode
- OpenSSL Certificate Verification Depth
- Policy Evaluation Realm
- Policy Set
- POST Data Storage Directory
- Private Client Certificate File Name
- Private Key Password
- Proxy Server Host Name
- Proxy Server Password
- Proxy Server Port
- Proxy Server User
- Public Client Certificate File Name
- Remove IIS HTTP Server Header
- Security Protocol List
- Server Certificate Trust
- Supported Cipher List
- TCP Receive Timeout
- Use Cached Configuration After Update
- Web Socket Connection Interval

## Properties by function

The agent configurations support properties that have the following functions.

### *Advice handling*

- Composite Advice Encode
- Composite Advice Handling

### *Agent profile*

- [Agent Profile Password](#)
- [Agent Profile Realm](#)
- [Agent Profile Password Encryption Key](#)
- [Agent Profile Name](#)

### *Attribute processing*

- [Attribute Multi-Value Separator](#)
- [Profile Attribute Fetch Mode](#)
- [Session Attribute Map](#)
- [Response Attribute Map](#)
- [Response Attribute Fetch Mode](#)
- [Session Attribute Fetch Mode](#)
- [Profile Attribute Map](#)

### *Audit*

- [Audit Access Types](#)
- [Audit Log Location](#)
- [Local Agent Audit File Name](#)

### *Client identification*

- [Anonymous User](#)
- [Client Hostname Header](#)
- [Client IP Address Header](#)

### *Connection pooling*

- [Enable Connection Pooling](#)

### *Continuous Security*

- [Continuous Security Cookie Map](#)
- [Continuous Security Header Map](#)

### *Cookies*

- [Accept SSO Token](#)

- [Persist JWT Cookie](#)
- [Enable Cookie Security](#)
- [SameSite Cookie Attribute](#)
- [Cookie Reset List](#)
- [Encode Special Characters in Cookies](#)
- [Enable Multivalued for Pre-Authn Cookie](#)
- [Profile Attribute Cookie Prefix](#)
- [Cookie Name](#)
- [Profile Attributes Cookie Maxage](#)
- [Enable HTTP Only Mode](#)
- [Enable Cookie Reset](#)

### *Cross-domain single sign-on*

- [Enable Session Cookie Reset After Authentication Redirect](#)
- [CDSSO Redirect URI](#)
- [Cookie Domain List](#)

### *Custom*

- [Custom Properties](#)

### *Debug*

- [Agent Debug Level](#)
- [Agent Debug File Size](#)

### *Encryption*

- [Server Certificate Trust](#)
- [Private Client Certificate File Name](#)
- [Supported Cipher List](#)
- [Accept Secure Cookies From AM Over HTTP](#)
- [Public Client Certificate File Name](#)
- [CA Certificate File Name](#)
- [Private Key Password](#)
- [Enable OpenSSL to Secure Internal Communications](#)

- [OpenSSL Certificate Verification Depth](#)

### *FQDN check*

- [FQDN Virtual Host Map](#)
- [Enable FQDN Check](#)
- [FQDN Default](#)

### *Forward proxy*

- [Proxy Server Password](#)
- [Proxy Server Port](#)
- [Proxy Server User](#)
- [Proxy Server Host Name](#)

### *Fragment redirect*

- [Enable Fragment Redirect](#)

### *General*

- [Enable SSO Only Mode](#)
- [Reset Idle Timeout](#)
- [Hostname to IP Address Map](#)
- [Resources Access Denied URL](#)

### *Goto parameter*

- [Goto Parameter Name](#)

### *Headers*

- [MIME-Encode HTTP Header Values](#)
- [Add Cache-Control Headers](#)

### *Ignore path info*

- [Ignore Path Info in Request URLs](#)

### *JSON-formatted response*

- [List of URLs to Receive JSON-Formatted Responses](#)
- [Invert Properties That Receive JSON-Formatted Responses](#)
- [Headers and Values to Receive JSON-Formatted Responses](#)
- [HTTP Return Code for JSON-Formatted Responses](#)

### *Load balancing*

- [Enable Override Request URL Host](#)
- [Enable Override Request URL Port](#)
- [Enable Override Request URL Protocol](#)
- [POST Data Sticky Load Balancing Value](#)
- [Enable AM Load Balancer Cookie](#)
- [POST Data Sticky Load Balancing Mode](#)

### *Login URL*

- [Public AM URL](#)

### *Login redirect*

- [AM Conditional Login URL](#)
- [Authorization flow for applications using Javascript](#)
- [Regular Expression Conditional Login URL](#)
- [AM Login URL](#)
- [Regular Expression Conditional Login Pattern](#)
- [Enable Custom Login Mode](#)

### *Logout redirect*

- [Disable Logout Redirection](#)
- [Logout URL List](#)
- [Enable Regex for Logout URL List](#)
- [Enable Invalidate Logout Session](#)
- [Agent Logout URL Regular Expression](#)
- [AM Logout URL](#)
- [Reset Cookies on Logout List](#)
- [Logout Redirect URL](#)

## *Logs*

- [Local Audit Log Rotation Size](#)
- [Local Agent Debug File Name](#)
- [Maximum Number of Debug Log Files](#)

## *Microsoft IIS server*

- [Show Password in HTTP Header](#)
- [Logon and Impersonation](#)
- [Remove IIS HTTP Server Header](#)
- [Replay Password Key](#)

## *Miscellaneous*

- [TCP Receive Timeout](#)
- [AM Connection URL](#)
- [Connection Timeout](#)
- [Security Protocol List](#)
- [Use Built-in Apache HTTPD Authentication Directives](#)

## *Not-enforced*

- [Ignore Path Info in Not-Enforced URLs](#)
- [Regular Expressions for Not-Enforced URLs](#)
- [Enable Regular Expressions for Not-Enforced IPs](#)
- [Not-Enforced Fallback Mode](#)
- [Client IP Validation](#)
- [Invert Not-Enforced URLs](#)
- [Not-Enforced URL List](#)
- [Fetch Attributes for Not-Enforced URLs](#)
- [Not-Enforced IP List](#)
- [Not-Enforced URL from IP Processing List](#)

## *POST data preservation*

- [Enable POST Data Preservation](#)

- [POST Data Entries Cache Period](#)
- [POST Data Storage Directory](#)
- [URLs Ignored by the POST Data Inspector](#)
- [Submit POST Data using JavaScript](#)

### *Policy client service*

- [User ID Parameter](#)
- [Policy Cache Polling Period](#)
- [Policy Clock Skew](#)
- [Policy Evaluation Realm](#)
- [Fetch Policies From The Root Resource](#)
- [Enable Retrieve Client Hostname](#)
- [SSO Cache Polling Period](#)
- [User ID Parameter Type](#)
- [Policy Set](#)

### *Profile*

- [Accept SSO token cookie \(deprecated\)](#)
- [Agent Profile ID Allow List](#)
- [Web Socket Connection Interval](#)
- [Enable Notifications of Agent Configuration Change](#)
- [Configuration Reload Interval](#)
- [Agent Root URL for CDSSO](#)
- [Disable Audience Claim Validation](#)
- [JWT Cookie Name](#)
- [Password](#)
- [Location of Agent Configuration Repository](#)
- [Retain Session Cache After Configuration Change](#)
- [Agent Deployment URI Prefix](#)
- [Use Cached Configuration After Update](#)
- [Enable Notifications](#)
- [Group](#)



## URL handling

- [Encode Special Characters in URLs](#)
- [Enable URL Comparison Case Sensitivity Check](#)
- [Invalid URL Regular Expression](#)

## Advice handling

### Composite Advice Encode

---

A flag for whether to base64 URL-encode composite advices before sending them to custom login endpoints:

`true` : Advices are encoded to increase the security, and protect against cross-site scripting attacks.

`false` : Advices are not encoded

Default: `false`

Property name	<code>com.forgerock.agents.advice.b64.url.encode</code> Introduced in Web Agent 5.7
Type	Boolean: <code>true</code> returns true; all other strings return <code>false</code> .
Bootstrap property	No
Required property	No
Restart required	No
AM console	Tab: Miscellaneous (From AM 7)  Title: Composite Advice Encode

### Composite Advice Handling

---

When `true`, the agent sends composite advice in the query (GET request) instead of sending it through a POST request.

Default: `false`

Property name	com.sun.am.use_redirect_for_advice Introduced in Web Agent 4.x
Type	Boolean: true returns true; all other strings return false.
Bootstrap property	No
Required property	No
Restart required	No
AM console	Tab: Miscellaneous (From AM 7) Title: Composite Advice Handling

## Agent profile

### Agent Profile Password

---

The password required by the agent profile, encrypted with the key specified in [Agent Profile Password Encryption Key](#).

To encrypt an agent profile password, run the `agentadmin` command with the `--p` option.

Default: Empty

Property name	com.sun.identity.agents.config.password Introduced in Web Agent 4.x
Type	String
Bootstrap property	Yes
Required property	No
Restart required	No

### Agent Profile Realm

---

The AM realm where the agent profile is located. For example, `/Customers`.

Realm names are case-sensitive. Failure to set the realm name exactly as configured in AM causes the agent to fail to recognize the realm.

Default: /

Property name	com.sun.identity.agents.config.organization.name Introduced in Web Agent 4.x
Type	String
Bootstrap property	Yes
Required property	No
Restart required	No

## Agent Profile Password Encryption Key

---

The encryption key used to encrypt the agent profile password, which should be provided in [Agent Profile Password](#).

To create a encryption key, run the **agentadmin** command with the `--k` option.

Default: Empty

Property name	com.sun.identity.agents.config.key Introduced in Web Agent 4.x
Type	String
Bootstrap property	Yes
Required property	No
Restart required	No

## Agent Profile Name

---

The name of the agent profile in AM.

Property name	com.sun.identity.agents.config.username Introduced in Web Agent 4.x
Type	String

Bootstrap property	Yes
Required property	No
Restart required	No

## Attribute processing

### Attribute Multi-Value Separator

---

The separator between values in a multi-valued attribute. The separator applies to all attributes, such as profile, session, and response attributes.

In this example, the attribute `HTTP_CUSTOM_TEL` has two values separated by a pipe (`|`):

```
HTTP_CUSTOM_TEL = 45354345|1234
```

Note: If you use custom code to construct a multi-valued attribute, make sure that the attribute is a string containing the individual values separated by this parameter.

Default: `|`

Property name	<code>com.sun.identity.agents.config.attribute.multi.value.separator</code> Introduced in Web Agent 4.x
Type	String
Bootstrap property	No
Required property	No
Restart required	No
AM console	Tab: Application  Title: Attribute Multi-Value Separator

### Profile Attribute Fetch Mode

---

Map profile attributes to HTTP headers or HTTP cookies:

```
HTTP_COOKIE : Map to HTTP cookies
```

HTTP\_HEADER: Map to HTTP headers

Default: NONE

Property name	<code>com.sun.identity.agents.config.profile.attribute.fetch.mode</code> Introduced in Web Agent 4.x
Type	Constrained Values: "http_header", "http_cookie", "none"
Bootstrap property	No
Required property	No
Restart required	No
AM console	Tab: Application  Title: Profile Attribute Fetch Mode

## Session Attribute Map

Map the value of a specified session attribute to one or more HTTP headers or HTTP cookies, depending on the value of Session Attribute Fetch Mode.

- Map key: The name of an existing session attribute for the currently authenticated user.
- Map value: The name of one or more HTTP headers or HTTP cookies.

If the HTTP header or HTTP cookie name does not exist, the agent creates it. If the session attribute name (key) does not exist, the agent does not create the HTTP header or HTTP cookie.

### NOTE

Underscores in header names can cause errors in some web containers. Either don't use underscores in header names, or see your web container documentation for information about how they are managed.

When an HTTP header name is used in a request header, it is prefixed by `HTTP_`. The agents automatically changes lower case letters to upper case, and hyphens ( - ) to underscores ( \_ ). For example, `CUSTOM-userid` becomes `HTTP_CUSTOM-USERID`.

Format:

```
com.sun.identity.agents.config.session.attribute.mapping[session_attribute]=  
ATTR1|ATTR2
```

Examples:

The following example maps the value of the session attribute `UserToken` to the HTTP header `CUSTOM-userid`:

```
com.sun.identity.agents.config.session.attribute.mapping[UserToken]=CUSTOM-userid.
```

The following example maps the value of the session attribute `UserId` to two HTTP headers:

```
com.sun.identity.agents.config.session.attribute.mapping[UserId]=HEADER1|HEADER2`.
```

Default: Empty

Property name	<code>com.sun.identity.agents.config.session.attribute.mapping</code> Introduced in Web Agent 4.x
Type	String Map
Bootstrap property	No
Required property	No
Restart required	No
AM console	Tab: Application Title: Session Attribute Map

## Response Attribute Map

---

Map the value of a specified response attribute to one or more HTTP headers or HTTP cookies, depending on the value of [Response Attribute Fetch Mode](#).

- Map key: The name of a response attribute returned by AM with a policy decision.
- Map value: The name of one or more HTTP headers or HTTP cookies.

Consider the following points for cookies:

- If an HTTP cookie with the mapped name does not exist, the agent creates it.
- If an HTTP cookie with the mapped name already exists, the agent recreates it.
- If an unauthenticated user attempts to access the protected page, the agent deletes HTTP cookies with the mapped name on the first request, and then creates them

after login.

- If the profile attribute name (key) does not exist, the agent does not create the HTTP cookie.

Consider the following points for response headers:

- If a response header with the mapped name does not exist, the agent creates it.
- If an HTTP cookie with the mapped name already exists, the agent does not recreates it, it simply appends information to the header.
- If the profile attribute name (key) does not exist, the agent does not create the response header.
- Underscores in header names can cause errors in some web containers. Either don't use underscores in header names, or see your web container documentation for information about how they are managed.
- When an HTTP header name is used in a request header, it is prefixed by `HTTP_`. The agents automatically changes lower case letters to upper case, and hyphens ( - ) to underscores ( \_ ). For example, `CUSTOM-userid` becomes `HTTP_CUSTOM-USERID`.

Format: response attribute = HEADER-NAME(S)

Examples:

In the following example, the AM response attribute `uid` is mapped to `CUSTOM-User-Name`: `com.sun.identity.agents.config.response.attribute.mapping[uid]=Custom-User-Name`

Default: Empty

Property name	<code>com.sun.identity.agents.config.response.attribute.mapping</code> Introduced in Web Agent 4.x
Type	String Map
Bootstrap property	No
Required property	No
Restart required	No
AM console	Tab: Application Title: Response Attribute Map

## Response Attribute Fetch Mode

---

Map response attributes to HTTP headers or HTTP cookies:

HTTP\_COOKIE : Map to HTTP cookies

HTTP\_HEADER : Map to HTTP headers

Default: NONE

Property name	<code>com.sun.identity.agents.config.response.attribute.fetch.mode</code> Introduced in Web Agent 4.x
Type	Constrained Values: "http_header", "http_cookie", "none"
Bootstrap property	No
Required property	No
Restart required	No
AM console	Tab: Application  Title: Response Attribute Fetch Mode

## Session Attribute Fetch Mode

---

Map session attributes to HTTP headers or HTTP cookies:

HTTP\_COOKIE : Map to HTTP cookies

HTTP\_HEADER : Map to HTTP headers

Default: NONE

Property name	<code>com.sun.identity.agents.config.session.attribute.fetch.mode</code> Introduced in Web Agent 4.x
Type	Constrained Values: "http_header", "http_cookie", "none"
Bootstrap property	No
Required property	No



Restart required	No
AM console	Tab: Application Title: Session Attribute Fetch Mode

## Profile Attribute Map

Map the value of a specified profile attribute to one or more HTTP headers or HTTP cookies, depending on the value of Profile Attribute Fetch Mode.

- Map key: The name of an existing profile attribute for the currently authenticated user.
- Map value: The name of one or more HTTP headers or HTTP cookies.

If the HTTP header or HTTP cookie name does not exist, the agent creates it. If the profile attribute name (key) does not exist, the agent does not create the HTTP header or HTTP cookie.

### NOTE

Underscores in header names can cause errors in some web containers. Either don't use underscores in header names, or see your web container documentation for information about how they are managed.

To populate the value of profile attribute CN under `CUSTOM-Common-Name`, configure `com.sun.identity.agents.config.profile.attribute.mapping[CN]=CUSTOM-Common-Name`.

### TIP

Make sure the case of your LDAP attribute name matches the case of the LDAP schema, otherwise you may see an error similar to the following: `do_header_set(): SM_LOGIN (UiD) is not available in profile attributes`

In most cases, in a destination 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, `CUSTOM-userid` becomes `HTTP_CUSTOM-USERID`.

Format: `profile attribute = HEADER-NAME(S)`

Example: `[CN]=HEADER1|HEADER2`

Default: Empty

Property name	com.sun.identity.agents.config.profile.attribute.mapping Introduced in Web Agent 4.x
Type	String Map
Bootstrap property	No
Required property	No
Restart required	No
AM console	Tab: Application  Title: Profile Attribute Map

## Audit

### Audit Access Types

---

The type of audit events to log:

- LOG\_NONE : Disable audit logging.
- LOG\_ALLOW : Log access allowed events.
- LOG\_DENY : Log access denied events.
- LOG\_BOTH : Log access allowed and access denied events.

Default: LOG\_NONE

Property name	com.sun.identity.agents.config.audit.accesstype Introduced in Web Agent 4.x
Type	Constrained Values: "local", "remote", "both"
Bootstrap property	No
Required property	No
Restart required	No
AM console	Tab: Global  Title: Audit Access Types

# Audit Log Location

---

The location where the agent logs audit messages:

- REMOTE : Log audit event messages to the audit event handler configured in the AM realm where the web agent is configured.
- LOCAL : Log audit event messages locally to the agent installation.
- ALL : Log audit event messages to the audit event handler configured in the AM realm and locally to the agent installation.

Default: REMOTE

Property name	com.sun.identity.agents.config.log.disposition Introduced in Web Agent 4.x
Type	String
Bootstrap property	No
Required property	No
Restart required	No
AM console	Tab: Global  Title: Audit Log Location

# Local Agent Audit File Name

---

If Audit Log Location is LOCAL or ALL , this property gives the name of the local file that contains agent audit messages.

Default: /web\_agents/agent\_type/instances/agent\_nnn/logs/audit/audit.log

Property name	com.sun.identity.agents.config.local.audit.logfile Introduced in Web Agent 4.x
Type	String
Bootstrap property	Yes
Required property	No

Restart required	No
------------------	----

## Client identification

### Anonymous User

---

Enable or disable REMOTE\_USER processing for anonymous users.

Default: false

Property name	com.sun.identity.agents.config.anonymous.user.enable Introduced in Web Agent 4.x
Type	Boolean: true returns true; all other strings return false.
Bootstrap property	No
Required property	No
Restart required	No
AM console	Tab: Miscellaneous Title: Anonymous User

### Client Hostname Header

---

Name of the HTTP header that holds the hostname of the client.

Default: Empty

Property name	com.sun.identity.agents.config.client.hostname.header Introduced in Web Agent 4.x
Type	String
Bootstrap property	No
Required property	No

Restart required	No
AM console	Tab: Advanced Title: Client Hostname Header

## Client IP Address Header

---

Name of the HTTP header that holds the IP address of the client.

Default: Empty

Property name	<code>com.sun.identity.agents.config.client.ip.header</code> Introduced in Web Agent 4.x
Type	String
Bootstrap property	No
Required property	No
Restart required	No
AM console	Tab: Advanced Title: Client IP Address Header

## Connection pooling

### 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.

Default: `true`

Property name	<code>org.forgerock.agents.config.connection.pool.enable</code> Introduced in Web Agent 5.8
Type	Boolean: <code>true</code> returns true; all other strings return <code>false</code> .
Bootstrap property	Yes
Required property	No
Restart required	No

## Continuous Security

### Continuous Security Cookie Map

Map of cookie name to entry in the environmental conditions map, used during policy evaluation:

- Map key: Cookie name in the inbound request
- Map value: Name of the entry in the environmental conditions map that contains the value of `cookie_name`

This property has the format `[cookie_name]=map_entry_name`, where:

Example:

```
org.forgerock.openam.agents.config.continuous.security.cookies[trackingcookie1]=myCookieEntry
```

Default: Empty

Property name	<code>org.forgerock.openam.agents.config.continuous.security.cookies</code> Introduced in Web Agent 4.x
Type	String Map
Bootstrap property	No
Required property	No
Restart required	No

AM console	Tab: Application Title: Continuous Security Cookie Map
------------	---

## Continuous Security Header Map

---

Map of header name to entry in the environmental conditions map, used during policy evaluation:

- Map key: Header name in the inbound request
- Map value: Name of the entry in the environmental conditions map that contains the value of the header name

Example:

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

Default: Empty

Property name	org.forgerock.openam.agents.config.continuous.security.headers Introduced in Web Agent 4.x
Type	String Map
Bootstrap property	No
Required property	No
Restart required	No
AM console	Tab: Application Title: Continuous Security Header Map

## Cookies

### Accept SSO Token

---

A flag for whether the agent accepts SSO tokens and ID tokens as session cookies:

- `0`. The agent does not accept SSO tokens as session cookies.

- 1 . The agent accepts both SSO tokens and ID tokens as session tokens during the login flow, and afterwards. SSO tokens *are not converted* to ID tokens. Set this property to 1 only for environments migrating from earlier versions of the agent, in the following scenarios:
  - Your custom login pages use SSO tokens as session tokens, and [Enable Custom Login Mode](#) is set to 2 .
  - Your applications, for example, REST or JavaScript clients, can only set SSO tokens.

The SSO token name is given by [Cookie Name](#).

If the agent receives a request with both an SSO token and an ID token, it checks the ID token first. If invalid, it checks the SSO token. If both are invalid, the agent redirects the user for authentication.

The agent caches session information for SSO tokens.

Configure this property with [Enable Custom Login Mode](#), as described in [Login redirect configuration options](#) in the *User Guide*.

Default: 0

Property name	com.forgerock.agents.accept.sso.token Introduced in Web Agent 5.7
Type	Integer
Bootstrap property	No
Required property	No
Restart required	No
AM console	Tab: SSO  Title: Accept SSO Token

## Persist JWT Cookie

---

A flag to persist JWT cookies. If `true` the JWT cookie is not set as a Session Cookie.

Default: `false`



Property name	<code>org.forgerock.agents.config.cdsso.persistent.cookie.enable</code> Introduced in Web Agent 4.x
Type	Boolean: <code>true</code> returns true; all other strings return <code>false</code> .
Bootstrap property	No
Required property	No
Restart required	No
AM console	Tab: SSO (From AM 7)  Title: Persist JWT Cookie

## Enable Cookie Security

---

When `true`, the agent marks cookies as secure, sending them only if the communication channel is secure. Set to `true` when agent connections are over SSL.

Default: `false`

Property name	<code>com.sun.identity.agents.config.cookie.secure</code> Introduced in Web Agent 4.x
Type	Integer
Bootstrap property	No
Required property	No
Restart required	No
AM console	Tab: SSO  Title: Enable Cookie Security

## SameSite Cookie Attribute

---

Sets the `SameSite` attribute on all the cookies that it creates. The value of the `SameSite` attribute is what you configure in this property.

For example, to add the `SameSite` attribute with the value of `Lax` to the cookies, set this property to `Lax`.

The attribute is not set for some browsers and circumstances, as described in <https://www.chromium.org/updates/same-site/incompatible-clients>.

Default: Empty

Property name	<code>com.forgerock.agents.cdsso.cookie.samesite</code> Introduced in Web Agent 5.7
Type	String
Bootstrap property	No
Required property	No
Restart required	No
AM console	Tab: SS0  Title: SameSite Cookie Attribute

## Cookie Reset List

---

List of cookies to reset. For example:

```
com.sun.identity.agents.config.cookie.reset[0]=myCookie
```

```
com.sun.identity.agents.config.cookie.reset[1]=nextCookie
```

Default: Empty

Property name	<code>com.sun.identity.agents.config.cookie.reset</code> Introduced in Web Agent 4.x
Type	String Map
Bootstrap property	No
Required property	No
Restart required	No
AM console	Tab: SS0  Title: Cookie Reset List

## Encode Special Characters in Cookies

---

When `true`, use URL encoding for special characters in cookies. This is useful when profile, session, and response attributes contain special characters, and the attributes fetch mode is set to `HTTP_COOKIE`.

Default: `false`

Property name	<code>com.sun.identity.agents.config.encode.cookie.special.chars.enable</code> Introduced in Web Agent 4.x
Type	Boolean: <code>true</code> returns true; all other strings return <code>false</code> .
Bootstrap property	No
Required property	No
Restart required	No
AM console	Tab: Miscellaneous Title: Encode Special Characters in Cookies

## Enable Multivalued for Pre-Authn Cookie

---

Web agent uses the pre-authentication cookie `agent-authn-tx` to track the progress of authentication with AM and protect the request from replay attacks.

When this property is `true`, 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.

When this property is `false`, the agent creates a pre-authentication cookie for each authentication request to AM, with the name of `agent-authn-tx-string`.

In some environments, this will create 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 have a limit of how many cookies they can handle.

Something similar happens to web servers; they have a limit of how many headers (cookies) they can manage at one time. Set the property to `true` if you find that creating too many cookies is having an impact on your environment.

Default: `false`

Property name	<code>org.forgerock.openam.agents.config.multivalue.pre.authn.cookies</code> Introduced in Web Agent 5.7
Type	Boolean: <code>true</code> returns true; all other strings return <code>false</code> .
Bootstrap property	Yes
Required property	No
Restart required	No
AM console	Tab: SSO (From AM 7)  Title: Enable Multivalue for Pre-Authn Cookie

## Profile Attribute Cookie Prefix

---

A prefix for the cookie attributes headers.

Default: `HTTP_`

Property name	<code>com.sun.identity.agents.config.profile.attribute.cookie.prefix</code> Introduced in Web Agent 4.x
Type	String
Bootstrap property	No
Required property	No
Restart required	No
AM console	Tab: Miscellaneous  Title: Profile Attribute Cookie Prefix

## Cookie Name

---

Name of the SSO token cookie used for authentication with AM. If empty, the agent retrieves the cookie name from the AM server.

Default: `iPlanetDirectoryPro`

Property name	<code>com.sun.identity.agents.config.cookie.name</code> Introduced in Web Agent 4.x
Type	String
Bootstrap property	No
Required property	No
Restart required	No
AM console	Tab: SSO  Title: Cookie Name

## Profile Attributes Cookie Maxage

---

Number of seconds before expiration of custom cookies or the pre-authentication cookie, `agent-authn-tx`.

Pre-authentication cookies expire when the first of the following events occurs:

- Authentication completes successfully
- They reach the age configured by this property

If POST data preservation is enabled, the request expires after the time specified in [POST Data Entries Cache Period](#), which is by default 10 minutes. In this case, consider increasing the value of this property to at least 600 seconds.

Default: `300`

Property name	<code>com.sun.identity.agents.config.profile.attribute.cookie.maxage</code> Introduced in Web Agent 4.x
Type	Integer
Bootstrap property	No

Required property	No
Restart required	No
AM console	Tab: Miscellaneous Title: Profile Attributes Cookie Maxage

## Enable HTTP Only Mode

---

When `true`, mark cookies as `HttpOnly` to prevent scripts and third-party software from accessing them.

Default: `true`

Property name	<code>com.sun.identity.cookie.httponly</code> Introduced in Web Agent 4.x
Type	Boolean: <code>true</code> returns <code>true</code> ; all other strings return <code>false</code> .
Bootstrap property	No
Required property	No
Restart required	No
AM console	Tab: SSO (From AM 7) Title: Enable HTTP Only Mode

## Enable Cookie Reset

---

When `true`, the agent resets (blanks) cookies in the response before redirecting to authentication by issuing a `Set-Cookie` header to the client. An example header could be similar to this:

```
Set-Cookie myCookie= ; Max-Age=0; Expires=Thu, 01-Jan-1970 00:00:00 GMT;
Domain=.my.default.fqdn
```

If [FQDN Default](#) is set, the agent sets the cookie domain to the domain specified by the property. Otherwise, the agent leaves the cookie domain blank.

Default: `false`

Property name	<code>com.sun.identity.agents.config.cookie.reset.enable</code> Introduced in Web Agent 4.x
Type	Boolean: <code>true</code> returns true; all other strings return <code>false</code> .
Bootstrap property	No
Required property	No
Restart required	No
AM console	Tab: SS0  Title: Enable Cookie Reset

## Cross-domain single sign-on

### Enable Session Cookie Reset After Authentication Redirect

---

Flag to reset the session cookie after an authentication redirect:

`true` : The agent does not reset the session cookie if a policy advice is present.

`false` : The agent resets the session cookie in all configured domains on every authentication redirect when a policy advice is present.

Default: `false`

Property name	<code>org.forgerock.agents.config.cdssso.advice.cleanup.disable</code> Introduced in Web Agent 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

AM console	Tab: SSO (From AM 7)  Title: Enable Session Cookie Reset After Authentication Redirect
------------	--

## CDSSO Redirect URI

---

Renames the endpoint the agent uses to process CDSSO requests. The name you choose for a production environment should not give away its purpose to end users.

The agent uses this endpoint during the default login redirection flow, but not during the custom login redirection flow.

Default: `agent/cdsso-oauth2`

Property name	<code>com.sun.identity.agents.config.cdsso.redirect.uri</code> Introduced in Web Agent 4.x
Type	String
Bootstrap property	No
Required property	No
Restart required	No
AM console	Tab: SSO  Title: CDSSO Redirect URI

## Cookie Domain List

---

List of domains, such as `.example.com`, in which cookies have to be set in CDSSO. If this property empty, then the fully qualified domain name of the cookie for the agent server is used to set the cookie domain, meaning that a host cookie rather than a domain cookie is set.

To set the list to `.example.com`, and `.example.net` using the configuration file property, include the following:

```
com.sun.identity.agents.config.cdsso.cookie.domain[0]=.example.com
```

```
com.sun.identity.agents.config.cdsso.cookie.domain[1]=.example.net
```



Default: Empty

Property name	<code>com.sun.identity.agents.config.cdsso.cookie.domain</code> Introduced in Web Agent 4.x
Type	String Map
Bootstrap property	No
Required property	No
Restart required	No
AM console	Tab: SS0  Title: Cookie Domain List

## Custom

## Custom Properties

---

Additional properties to augment the set of properties supported by agent. Custom properties can be specified as follows:

- `customproperty=custom-value1`
- `customlist[0]=customlist-value-0`
- `customlist[1]=customlist-value-1`
- `custommap[key1]=custommap-value-1`
- `custommap[key2]=custommap-value-2`

Add any property that is not yet in the AM console as a custom property.

Property name	<code>com.sun.identity.agents.config.freeformproperties</code> Introduced in Web Agent 4.x
Type	Unused
Bootstrap property	No
Required property	No
Restart required	No

AM console	Tab: Advanced Title: Custom Properties
------------	---

## Debug

### Agent Debug Level

Debug level. Set to one of the constrained values.

Default: Error

Property name	com.sun.identity.agents.config.debug.level Introduced in Web Agent 4.x
Type	Constrained Values: "info", "warning", "error", "debug", "all"
Bootstrap property	Yes
Required property	No
Restart required	No
AM console	Tab: Global Title: Agent Debug Level

### Agent Debug File Size

File size in bytes at which the debug log file is rotated.

Default: 0, debug log file is never rotated

Property name	com.sun.identity.agents.config.debug.file.size Introduced in Web Agent 4.x
Type	Integer
Bootstrap property	Yes
Required property	No

Restart required	No
AM console	Tab: Global (From AM 7.1) Title: Agent Debug File Size

## Encryption

### Server Certificate Trust

---

A flag to validate the certificate presented during SSL handshakes by the container where AM runs:

- `true`: The agent trusts any server certificate. By default, and to facilitate integration and testing, agent is configured to trust any server certificate.
- `false`: The agent trusts AM's certificate only if found to be correct and valid.

#### IMPORTANT

If the agent cannot connect to AM, it does not allow access to any protected resource. Ensure the agent is properly configured before setting this property to `false`.

Default: `true`

Property name	<code>com.sun.identity.agents.config.trust.server.certs</code> Introduced in Web Agent 4.x
Type	Boolean: <code>true</code> returns true; all other strings return <code>false</code> .
Bootstrap property	Yes
Required property	No
Restart required	No

### Private Client Certificate File Name

---

When AM is configured for client-side certificate verification, set this property to the file that contains the client certificate private key.

Agents using OpenSSL must specify the private key as a PEM file. For example:  
`com.forgerock.agents.config.cert.key = /opt/certificates/client_key.pem`

Agents using the Windows built-in Secure Channel API should not configure this property.

Default: Empty

Property name	<code>com.forgerock.agents.config.cert.key</code> Introduced in Web Agent 4.x
Type	String
Bootstrap property	Yes
Required property	No
Restart required	No

## Supported Cipher List

---

A colon separated list of one or more ciphers to support, as defined in <http://www.openssl.org/docs/apps/ciphers.html>.

Property name	<code>com.forgerock.agents.config.ciphers</code> Introduced in Web Agent 4.x
Type	String
Bootstrap property	Yes
Required property	No
Restart required	No

## Accept Secure Cookies From AM Over HTTP

---

A flag to accept secure cookies.

When `true`, the agent accepts secure cookies from AM over HTTP. When `false`, the agent rejects them.

For requests that arrive over a secure channel, by default, AM upgrades cookies to secure. However, during internal communication with the agent, AM can send these secure cookies over HTTP.

NOTE

**NOTE**

It is best practice to use HTTPS for *all* connections to AM.

Default: false

Property name	<code>com.forgerock.agents.config.plain.channels.insecure</code> Introduced in Web Agent 5.7
Type	Integer
Bootstrap property	Yes
Required property	No
Restart required	No

## Public Client Certificate File Name

When AM is configured to perform client certificate validation, set this property to the name of the file that contains the client certificate chain.

Agents using OpenSSL libraries must specify the certificate chain as a PEM file. For example: `com.forgerock.agents.config.cert.file = /opt/certificates/pub_client.pem`

Agents using the Windows built-in Secure Channel API must choose one of the following options:

- Store the certificate chain and its private key as a Personal Information Exchange Format (PFX) file, then configure it in the agent property. You must also configure the Private Key Password property.
- Store the certificate locally in the Windows certificate store and configure the friendly name of the client certificate as it shows in Windows, in the agent property.

Default: Empty

Property name	<code>com.forgerock.agents.config.cert.file</code> Introduced in Web Agent 4.x
Type	String
Bootstrap property	Yes
Required property	No

Restart required	No
------------------	----

## CA Certificate File Name

---

When the agent is configured to validate server certificates (Server Certificate Trust is `false`), set this property to the file name that contains a certificate or chain of certificates.

The file should be PEM encoded. For example:

```
com.forgerock.agents.config.cert.ca.file = /opt/certificates/am_ca.pem
```

```
com.sun.identity.agents.config.trust.server.certs = false
```

Set this property only when the agent is using OpenSSL libraries. For agent using the Windows built-in Secure Channel API, add the appropriate certificates to the Windows certificate store.

Default: Empty

Property name	<code>com.forgerock.agents.config.cert.ca.file</code> Introduced in Web Agent 4.x
Type	String
Bootstrap property	Yes
Required property	No
Restart required	No

## Private Key Password

---

When AM is configured for client-side certificate verification, and the PEM file containing the client certificate private key is password-protected, set this property to the obfuscated password.

Obfuscate the password by using `agentadmin --p` command. For example:

```
$ /web_agents/agent-type/bin> ./agentadmin --p "Encryption Key" "cat cert_password.file"
```

Encrypted password value: `zck+6RKqjtc=`

Where Encryption Key is the value of Agent Profile Password Encryption Key.

Default: Empty

Property name	<code>com.forgerock.agents.config.cert.key.password</code> Introduced in Web Agent 4.x
Type	String
Bootstrap property	Yes
Required property	No
Restart required	No

## Enable OpenSSL to Secure Internal Communications

---

Flag for whether Windows-based agents use the Windows built-in Secure Channel API or OpenSSL to secure internal communication with AM:

- `true` : The agent uses OpenSSL.
- `false` : The agent uses the Windows built-in Secure Channel API.

Default: `false`

Property name	<code>org.forgerock.agents.config.secure.channel.disable</code> Introduced in Web Agent 4.x
Type	Boolean: <code>true</code> returns true; all other strings return <code>false</code> .
Bootstrap property	Yes
Required property	No
Restart required	No

## OpenSSL Certificate Verification Depth

---

(OpenSSL only) Specifies how deeply the agent verifies AM's server certificate before deciding the certificate is not valid.

The depth is the maximum number of CA certificates that are followed while verifying the server certificate. If the certificate chain is longer than allowed, the certificates above the limit are ignored.

The property accepts the following values:

- 0 : Only self-signed certificates are accepted.
- 1 : Client certificates can be self-signed or must be signed by a CA which is directly known to the agent container.
- 2 or more: A chain of the specified number of certificates, including the previous ones. For example, the value 5 allows certificates from level 0 to level 5.

This property is relevant only when server certificate validation is enabled (Server Certificate Trust is `false`).

Default: 9

Property name	<code>org.forgerock.agents.config.cert.verify.depth</code> Introduced in Web Agent 4.x
Type	Integer
Bootstrap property	Yes
Required property	No
Restart required	No

## FQDN check

## FQDN Virtual Host Map

---

Key:Value maps of incoming hostname to outgoing domain. The map key must be set; the map value can contain one or more \* wildcards. Map keys and values are case insensitive.

This property requires Enable FQDN Check to be `true`, and FQDN Default to be set to suitable default FQDN.

Examples:

```
com.sun.identity.agents.config.fqdn.mapping[agent.localtest.me]=agent.example.com
```

```
com.sun.identity.agents.config.fqdn.mapping[agent.localtest.me]=agent-*
```



```
com.sun.identity.agents.config.fqdn.mapping[agent.localtest.me]=agent--  
other-
```

```
com.sun.identity.agents.config.fqdn.mapping[agent.othertest.me]=other.examp  
le.com
```

For more information, see [FQDN checking](#) in the *User Guide*.

Property name	com.sun.identity.agents.config.fqdn.mapping Introduced in Web Agent 4.x
Type	String Map
Bootstrap property	No
Required property	No
Restart required	No
AM console	Tab: Global  Title: FQDN Virtual Host Map

## Enable FQDN Check

When `true`, the agent checks whether request URLs match values in [FQDN Default](#) and [FQDN Virtual Host Map](#).

Use this property to prevent the redirect of requests in the following scenarios:

- Where resource URLs differ from the FQDNs in AM policies, for example, in load balanced and virtual host environments.
- Where hostnames are virtual, allocated dynamically, or match a pattern, for example in a Kubernetes deployment.
- Where hostnames are partial.

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

Default: `false`

For more information, see [FQDN checking](#) in the *User Guide*.

Property name	com.sun.identity.agents.config.fqdn.check.enable Introduced in Web Agent 4.x
---------------	---

Type	Boolean: true returns true; all other strings return false .
Bootstrap property	No
Required property	No
Restart required	No
AM console	Tab: Global Title: Enable FQDN Check

## FQDN Default

---

The default FQDN to access resources. Set this property during agent installation, and change it only if necessary. Without this value, the web server can fail to start.

This property requires [Enable FQDN Check](#) to be true .

### NOTE

If you specify an FQDN in this property, also add it to the [Agent Root URL for CDSSO](#).

For more information, see [FQDN checking](#) in the *User Guide*.

Property name	com.sun.identity.agents.config.fqdn.default Introduced in Web Agent 4.x
Type	String
Bootstrap property	No
Required property	No
Restart required	No
AM console	Tab: Global Title: FQDN Default

## Forward proxy

## Proxy Server Password

---

When AM and the agent communicate through a web proxy server configured in forward proxy mode, and the proxy server has the agent authenticate using Basic Authentication, set this property to the agent's password.

Default: Empty

Property name	<code>com.sun.identity.agents.config.forward.proxy.password</code> Introduced in Web Agent 4.x
Type	String
Bootstrap property	Yes
Required property	No
Restart required	No

## Proxy Server Port

---

When AM and the agent communicate through a web proxy server configured in forward proxy mode, set this property to the proxy server port number.

Default: Empty

Property name	<code>com.sun.identity.agents.config.forward.proxy.port</code> Introduced in Web Agent 4.x
Type	Integer
Bootstrap property	Yes
Required property	No
Restart required	No

## Proxy Server User

---

When AM and the agent communicate through a web proxy server configured in forward proxy mode, and the proxy server has the agent authenticate using Basic Authentication, set this property to the agent's user name.

Default: Empty

Property name	<code>com.sun.identity.agents.config.forward.proxy.use</code> <code>r</code> Introduced in Web Agent 4.x
Type	String
Bootstrap property	Yes
Required property	No
Restart required	No

## Proxy Server Host Name

---

When AM and the agent communicate through a web proxy server configured in forward proxy mode, set this property to the proxy server host name.

Default: Empty

Property name	<code>com.sun.identity.agents.config.forward.proxy.hos</code> <code>t</code> Introduced in Web Agent 4.x
Type	String
Bootstrap property	Yes
Required property	No
Restart required	No

## Fragment redirect

### Enable Fragment Redirect

---

A flag to manage the browser's URL fragment during authentication, as follows:

- `false`: Remove the browser's URL fragment during authentication. For example, a request to `http://my.domain.com:8080/myapp/index.html#chapter-1` is authenticated and redirected to `http://my.domain.com:8080/myapp/index.html`. The fragment `#chapter-1` is lost.

- `true`: Save the browser's URL fragment during authentication. For example, a request to `http://my.domain.com:8080/myapp/index.html#chapter-1` is authenticated and redirected to the same URL. The fragment is not lost.

An extra redirect is incurred for all unauthenticated requests, to capture and process the URL fragment.

Fragment redirect is not possible for request URLs marked for JSON responses, usually for non-browser clients, such as JavaScript or other coded clients.

Default: `false`

Property name	<code>org.forgerock.agents.config.fragment.redirect.enable</code> Introduced in Web Agent 5.7
Type	Boolean: <code>true</code> returns true; all other strings return <code>false</code> .
Bootstrap property	Yes
Required property	No
Restart required	No
AM console	Tab: Advanced (From AM 7)  Title: Enable Fragment Redirect

## General

### Enable SSO Only Mode

A flag to enable SSO only mode:

- `true`: The agent manages only user authentication. The filter invokes the AM Authentication Service to verify the identity of the user. If the user's identity is verified, the user is issued a session token through AM's Session Service.
- `false`: The agent manages user authorization, by using the policy engine in AM.

**TIP**

In SSO-only mode, consider configuring [Reset Idle Timeout](#).

Default: `false`

Property name	<code>com.sun.identity.agents.config.sso.only</code> Introduced in Web Agent 4.x
Type	Boolean: <code>true</code> returns true; all other strings return <code>false</code> .
Bootstrap property	No
Required property	No
Restart required	No
AM console	Tab: Global (From AM 7) Title: Enable SSO Only Mode

## Reset Idle Timeout

---

A flag for whether an agent configured in SSO-only mode should refresh the user's session idle time when the user accesses a protected resource.

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

If the agent is configured in SSO-only mode, the session may unexpectedly expire in AM due to idle timeout before the user has finished accessing the application.

Set this property to `true` to refresh the timeout when the user performs an action.

When set to `true`, the agent makes an additional call to AM; this may cause a performance impact. Configure this property only if:

- The agent is configured in SSO-only mode
- User's sessions are timing out in AM because they are unexpectedly reaching the maximum idle timeout value.

Default: `false`

Property name	<code>com.forgerock.agents.call.session.refresh</code> Introduced in Web Agent 5.7
Type	Boolean: <code>true</code> returns true; all other strings return <code>false</code> .
Bootstrap property	No

Required property	No
Restart required	No
AM console	Tab: Global Title: Reset Idle Timeout

## Hostname to IP Address Map

---

Map of hostname to an IP address. The mapped hostname is automatically resolved to the IP address.

- Map key: Hostname
- Map value: IP address

Configure this property in `agent.conf` or in the `Advanced` tab of the XUI.

Format: `com.forgerock.agents.config.hostmap[0]=<Hostname>|<IP>`

Example: `com.forgerock.agents.config.hostmap[0]=am.localtest.me|10.199.0.2`

Property name	<code>com.forgerock.agents.config.hostmap</code> Introduced in Web Agent 5.0
Type	String List
Bootstrap property	Yes
Required property	No
Restart required	No
AM console	Tab: Advanced (From AM 7.2) Title: Hostname to IP Address Map

## Resources Access Denied URL

---

The URL of the customized access denied page. If empty, the agent returns an HTTP status of 403 (Forbidden). The URL can be absolute or relative.

The following values are not permitted:

- Wildcards

- The . directory specifier
- The .. directory specifier

Default: Empty

Property name	<code>com.sun.identity.agents.config.access.denied.url</code> Introduced in Web Agent 4.x
Type	String
Bootstrap property	No
Required property	No
Restart required	No
AM console	Tab: Global  Title: Resources Access Denied URL

## Goto parameter

### Goto Parameter Name

Renames the `goto` parameter. The agent appends the requested URL to the renamed parameter during redirection, after logout or after reaching an access denied page. Rename the parameter when your application requires a parameter other than `goto`.

Consider the following example:

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

A valid redirection URL using the `goto2` parameter may look similar to the following:

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

The URL appended to the `goto2` parameter is the URL that the user tried to access when the agent redirected the request to the `accessDenied.html` page. Note that you configure the access denied page using [Resources Access Denied URL](#).

This property also affects [AM Logout URL](#).

Default: `goto`

Property name	<code>com.sun.identity.agents.config.redirect.param</code> Introduced in Web Agent 4.x
---------------	---



Type	String
Bootstrap property	No
Required property	No
Restart required	No
AM console	Tab: Miscellaneous Title: Goto Parameter Name

## Headers

### MIME-Encode HTTP Header Values

---

MIME-encoding of HTTP header values:

- Empty or 0 : The agent MIME-encodes the value of HTTP headers if said value is a multi-byte Unicode string.
- 1 : The agent MIME-encodes the value of every HTTP header.
- 2 : The agent does not MIME-encode the value of any HTTP header.

Default: Empty

Property name	com.forgerock.agents.header.mime.encode Introduced in Web Agent 5.7
Type	Integer
Bootstrap property	No
Required property	No
Restart required	No
AM console	Tab: Miscellaneous (From AM 7) Title: MIME-Encode HTTP Header Values

### Add Cache-Control Headers

---

When `true`, enables the use of Cache-Control headers to prevent proxies from caching resources accessed by unauthenticated users.

Default: `false`

Property name	<code>com.forgerock.agents.cache_control_header.enable</code> Introduced in Web Agent 4.x
Type	Boolean: <code>true</code> returns <code>true</code> ; all other strings return <code>false</code> .
Bootstrap property	No
Required property	No
Restart required	No
AM console	Tab: Miscellaneous Title: Add Cache-Control Headers

## Ignore path info

### Ignore Path Info in Request URLs

---

When `true`, while doing the not-enforced list check and URL policy evaluation, strip path info from the request URL. Use this property to match to the URL without PATHINFO, as defined by the apache or IIS servers.

Example:

- If Not-Enforced URL List includes `http://host/*.gif`, then stripping path info from the request URI prevents access to `http://host/index.html` by using `http://host/index.html?hack.gif`.

However, when a web server is configured as a reverse proxy for a Java application server, the path info is interpreted to map a resource on the proxy server rather than the application server. This prevents the not-enforced list or the policy from being applied to the part of the URI below the application server path if a wildcard character is used.

Example:

- If Not-Enforced URL List includes `http://host/webapp/servlet/*` and the request URL is `http://host/webapp/servlet/example.jsp`, the path info is `/servlet/example.jsp`. When the path info stripped is, the resulting request URL is `http://host/webapp/`, which does not match the not-enforced list.

Therefore, when this property is enabled, path info is not stripped from the request URL even if there is a wildcard in the not-enforced list or policy.

When this property is `true`, make sure that nothing follows a wildcard in the not-enforced list or policy.

**NOTE**

The NGINX Plus Web Agent does not support this setting.

Default: `false`

Property name	<code>com.sun.identity.agents.config.ignore.path.info</code> Introduced in Web Agent 4.x
Type	Boolean: <code>true</code> returns true; all other strings return <code>false</code> .
Bootstrap property	No
Required property	No
Restart required	No
AM console	Tab: Miscellaneous  Title: Ignore Path Info in Request URLs

## JSON-formatted response

### List of URLs to Receive JSON-Formatted Responses

A list of resource URLs that trigger a JSON-formatted response from the agent, and, optionally, override the default HTTP status code.

Use this property for non-browser-based, or AJAX applications, that do not want to redirect users to the AM user interface for authentication.

**TIP**

Set the HTTP Return Code for JSON-Formatted Responses property to a supported HTTP code, for example `202`, to prevent applications that do not support redirects, for example, from displaying a default error page.

Example:

```
org.forgerock.agents.config.json.url[0]=http*://.example.com:/api/*
```

org.forgerock.agents.config.json.response.code=202

Performing a GET operation that matches the example triggers an HTTP result code 202 Accepted, and a JSON response containing 302 Found.

Default: Empty

Property name	org.forgerock.agents.config.json.url Introduced in Web Agent 4.x
Type	String Map
Bootstrap property	No
Required property	No
Restart required	No
AM console	Tab: Miscellaneous  Title: List of URLs to Receive JSON-Formatted Responses

## Invert Properties That Receive JSON-Formatted Responses

---

When `true`, the values specified in the following properties do not trigger JSON-formatted responses:

- [List of URLs to Receive JSON-Formatted Responses](#)
- [Headers and Values to Receive JSON-Formatted Responses](#)

Only non-specified values trigger JSON-formatted responses.

Default: `false`

Property name	org.forgerock.agents.config.json.url.invert Introduced in Web Agent 4.x
Type	Boolean: <code>true</code> returns true; all other strings return <code>false</code> .
Bootstrap property	No
Required property	No

Restart required	No
AM console	Tab: Miscellaneous (From AM 7)  Title: Invert Properties That Receive JSON-Formatted Responses

## Headers and Values to Receive JSON-Formatted Responses

Specify HTTP headers and associated values that trigger JSON-formatted errors to be returned.

Format:

```
org.forgerock.agents.config.json.header[Header]=Value
```

Use with [HTTP Return Code for JSON-Formatted Responses](#), as follows:

```
org.forgerock.agents.config.json.header[enableJsonResponse]=true
```

```
org.forgerock.agents.config.json.response.code=202
```

Performing a GET operation that matches the example triggers an HTTP result code 202 Accepted, and a JSON response containing 302 Found.

Default: Empty

Property name	org.forgerock.agents.config.json.header Introduced in Web Agent 4.x
Type	String Map
Bootstrap property	No
Required property	No
Restart required	No
AM console	Tab: Miscellaneous (From AM 7)  Title: Headers and Values to Receive JSON-Formatted Responses

# HTTP Return Code for JSON-Formatted Responses

---

An HTTP response code to return when a JSON-formatted error is triggered.

**TIP**

To prevent user agents displaying their default error pages, set to a non-error HTTP code, for example 202.

Example:

```
org.forgerock.agents.config.json.url[0]=http*://.example.com:/api/*
```

```
org.forgerock.agents.config.json.response.code=202
```

Performing a GET operation that matches the example triggers an HTTP result code 202 Accepted, and a JSON response containing 302 Found.

Default: Empty

Property name	org.forgerock.agents.config.json.response.code Introduced in Web Agent 4.x
Type	Integer
Bootstrap property	No
Required property	No
Restart required	No
AM console	Tab: Miscellaneous (From AM 7)  Title: HTTP Return Code for JSON-Formatted Responses

## Load balancing

## Enable Override Request URL Host

---

Enable if the agent is behind a SSL/TLS off-loader, load balancer, or proxy, where the users and the agent use a different host. When true, the host is overridden with the value from Agent Deployment URI Prefix.

When the following headers are defined on the proxy or load-balancer, they override the value of Agent Deployment URI Prefix:

- X-Forwarded-Proto
- X-Forwarded-Host
- X-Forwarded-Port

If you are using these headers, do not configure the agent to override its hostname, port, or protocol.

Default: false

Property name	com.sun.identity.agents.config.override.host Introduced in Web Agent 4.x
Type	Boolean: true returns true; all other strings return false .
Bootstrap property	No
Required property	No
Restart required	No
AM console	Tab: Advanced  Title: Enable Override Request URL Host

## Enable Override Request URL Port

---

Enable if the agent is behind a SSL/TLS off-loader, load balancer, or proxy, where the users and the agent use a different port. When true , the port is overridden with the value from Agent Deployment URI Prefix.

When the following headers are defined on the proxy or load-balancer, they override the value of Agent Deployment URI Prefix:

- X-Forwarded-Proto
- X-Forwarded-Host
- X-Forwarded-Port

If you are using these headers, do not configure the agent to override its hostname, port, or protocol.

Default: false

Property name	com.sun.identity.agents.config.override.port Introduced in Web Agent 4.x
Type	Boolean: true returns true; all other strings return false.
Bootstrap property	No
Required property	No
Restart required	No
AM console	Tab: Advanced  Title: Enable Override Request URL Port

## Enable Override Request URL Protocol

---

Enable if the agent is behind a SSL/TLS off-loader, load balancer, or proxy, where the users and the agent use a different protocol. When `true`, the protocol is overridden with the value from [Agent Deployment URI Prefix](#).

When the following headers are defined on the proxy or load-balancer, they override the value of [Agent Deployment URI Prefix](#):

- X-Forwarded-Proto
- X-Forwarded-Host
- X-Forwarded-Port

If you are using these headers, do not configure the agent to override its hostname, port, or protocol.

Default: `false`

Property name	com.sun.identity.agents.config.override.protocol Introduced in Web Agent 4.x
Type	Boolean: true returns true; all other strings return false.
Bootstrap property	No
Required property	No
Restart required	No



AM console	Tab: Advanced  Title: Enable Override Request URL Protocol
------------	--

## POST Data Sticky Load Balancing Value

A key-value pair separated by the equals (=) character that the agent creates when evaluating POST Data Sticky Load Balancing Mode.

For example, a setting of `lb=myserver` either sets an `lb` cookie with `myserver` value, or adds `lb=myserver` to the URL query string.

### NOTE

If this property is defined in the bootstrap agent configuration file (`agent.conf`), it overrides the property in the AM configuration.

Default: Empty

Property name	<code>com.sun.identity.agents.config.postdata.preserve.stickysession.value</code> Introduced in Web Agent 4.x
Type	String
Bootstrap property	No
Required property	No
Restart required	No
AM console	Tab: Advanced  Title: POST Data Sticky Load Balancing Value

## Enable AM Load Balancer Cookie

When `true`, the agent passes the hardcoded `amlbcookie` to AM.

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

Default: `false`

Property name	com.forgerock.agents.config.add.amlbcookie Introduced in Web Agent 5.8
Type	Boolean: true returns true; all other strings return false.
Bootstrap property	No
Required property	No
Restart required	No
AM console	Tab: Global (From AM 7.1)  Title: Enable AM Load Balancer Cookie

## POST Data Sticky Load Balancing Mode

Whether to create a cookie, or to append a query string to the URL to assist with sticky load balancing:

- **COOKIE** : The agent creates a cookie with the value specified in POST Data Sticky Load Balancing Value.
- **URL** : The agent appends the value specified in POST Data Sticky Load Balancing Value to the URL query string.

### NOTE

If this property is defined in the bootstrap agent configuration file (agent.conf), it overrides the property in the AM configuration.

Default: Empty

Property name	com.sun.identity.agents.config.postdata.preserve. .stickysession.mode Introduced in Web Agent 4.x
Type	String
Bootstrap property	No
Required property	No
Restart required	No

AM console	Tab: Advanced  Title: POST Data Sticky Load Balancing Mode
------------	--

## Login URL

## Public AM URL

The full URL of AM when it is behind a proxy during the custom login flow. For example, `protocol://public_am_fqdn:port/am`.

Use this property when both of the following points are true:

- Your environment uses custom login pages (non-OIDC-compliant flows), and the custom login pages are in a different domain than the agent.
- Your custom login pages are in a network that can only access AM using a proxy, a firewall, or any other technology that remaps the AM URL to one accessible by the custom login pages.

Consider an example where the traffic between AM and the agent happens through the `example-internal.com` domain, but the custom login pages are on the `example-external.com` domain. The traffic between the custom pages and AM translates `am.example-internal.com` into `am.example-external.com`. You would configure `https://am.example-external.com:8443/am` as the public AM URL.

Default: Empty

Property name	<code>com.forgerock.agents.public.am.url</code> Introduced in Web Agent 5.7
Type	String
Bootstrap property	No
Required property	No
Restart required	No
AM console	Tab: AM Services (From AM 7)  Title: Public AM URL

## Login redirect

# AM Conditional Login URL

---

Conditionally redirect users based on the incoming request 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.

Format, with no spaces between values:

```
[String] |[URL, URL...][?realm=value&module=value2&service=value3]
```

## **[String]**

Incoming login request URLs, with the following values:

- **Domain**: Agents match both the domain and its subdomains. For example, `example.com` matches `mydomain.example.com` and `www.example.com`. To combine domain and path, provide the port number: `www.example.com:8080/market`.
- **Subdomain**: For example, `example.com`. To combine subdomain and path, provide the port number: `example.com:8080/market`.
- **Path**: For example, `/myapp`.
- **Anything in the request URL**: For example, a port, such as `8080`.
- **No value**: Nothing is specified before the pipe ( `|` ) character. Conditional rules that do not specify the incoming request's domain apply to every incoming request.

To specify the string as a regular expression, configure the following properties instead: [Regular Expression Conditional Login Pattern](#) and [Regular Expression Conditional Login URL](#).

## **[URL, URL...]**

The URL to which incoming login requests are redirected. The URL can be the following:

- **AM instance or site**: Specify the URL of an AM instance or site in the format `protocol://FQDN[:port]/URI/oauth2/authorize`, where the port is optional if it is `80` or `443`. For example, `https://am.example.com/am/oauth2/authorize`.
- **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`.
- **List of AM instances or sites, or websites other than AM**: If the redirection URL is not specified, the agent redirects the request to the AM instance or site specified by [AM Connection URL](#).

### **?realm=/value**

The AM realm to where the agent should log the users. For example, ?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 sets the realm parameter, for example, because it lets the user chose it. In this case, ensure the custom login page always appends a realm parameter to the goto URL.
- The realm where the agent must log the user to has DNS aliases configured in AM. AM logs the user in to the realm whose DNS alias matches the incoming request URL. For example, an inbound request from `http://marketplace.example.com` URL logs into the marketplace realm if the realm alias is set to `marketplace.example.com`.
- The users should always log in to the top level realm.

If you specify the realm by default, this parameter can be overwritten by the custom login page if, for example, the user can chose the realm for authentication.

### **&module=value2&service=value3**

Parameters that can be added to the URL(s), such as:

- `module`: The authentication module the user authenticates against. For example, `?module=myAuthModule`.
- `service`: An authentication chain or tree the user authenticates against. For example, `?service=myAuthChain`.
- Any other parameters your custom login pages require.

Chain parameters with an ampersand (&) character, for example, `realm=value&service=value`.

When configuring conditional login with multiple URLs, set up the parameters for each URL.

Examples:

```
com.forgerock.agents.conditional.login.url[0]=example.com|https://am.example.com/am/oauth2/authorize
```

```
com.forgerock.agents.conditional.login.url[1]=myapp.domain.com|https://am2.example.com/am/oauth2/authorize?realm=/sales
```

```
com.forgerock.agents.conditional.login.url[3]=sales.example.com/marketplace|https://am1.example.com/am/oauth2/authorize?realm=/sales,https://am2.example.com/am/oauth2/authorize?realm=/marketplace
```

```
com.forgerock.agents.conditional.login.url[4]=myapp.domain.com|http://mylogin.example.com?realm=/customers
```

`com.forgerock.agents.conditional.login.url[5]=|https://am3.example.com/am/oauth2/authorize?realm=/customers&module=myAuthModule`

For more information, see [Login redirect](#) in the *User Guide*.

Property name	<code>com.forgerock.agents.conditional.login.url</code> Introduced in Web Agent 4.x
Type	String Map
Bootstrap property	No
Required property	No
Restart required	No
AM console	Tab: AM Services  Title: AM Conditional Login URL

## Authorization flow for applications using Javascript

### IMPORTANT

This feature is in Technology Preview, as defined in [Release levels and interface stability](#), for use only with assistance from Forgerock.

This property provides support for single page applications (SPAs) that use embedded login or authorization dialogs within `iframe` or `embed` tags.

Provide a JavaScript reference to a callback function, relative to the `iframe` or `embed` used for authentication dialogs with AM.

Use this property to enable callbacks into JavaScript applications after an authentication or transactional authorization journey.

Default: Empty

Property name	<code>com.forgerock.agents.config.auth.flow.callback</code> Introduced in Web Agent 5.10
Type	Unused
Bootstrap property	No
Required property	No

Restart required	No
AM console	Tab: Advanced  Title: Authorization flow for applications using Javascript

## Regular Expression Conditional Login URL

---

If the incoming request URL matches a pattern specified in [Regular Expression Conditional Login Pattern](#), the agent redirects the request to the specified URL.

The specific URL can be an AM instance, site, or a different website.

Example:

In the following example, when the request matches the regular expression `.*shop`, the agent redirects it to the `sales` realm for authentication:

```
org.forgerock.agents.config.conditional.login.pattern[0] = .*shop
```

```
org.forgerock.agents.config.conditional.login.url[0] =
http://am.example.com/am/oauth2/authorize?realm=sales
```

Default: Empty

Property name	<code>org.forgerock.agents.config.conditional.login.url</code> 1 Introduced in Web Agent 4.x
Type	String Map
Bootstrap property	No
Required property	No
Restart required	No
AM console	Tab: AM Services (From AM 7)  Title: Regular Expression Conditional Login URL

## AM Login URL

---

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

**IMPORTANT**

IMPORTANT

When redirecting incoming login requests to a custom login page, add the login page to [Not-Enforced IP List](#) or [Not-Enforced URL List](#).

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

- `URL` is the custom SSO-token-compliant login page to where the agent redirects the unauthenticated users.
- `[?realm=realm_name?parameter1=/value1&...]` specifies optional parameters that the agent will pass to the custom login page, for example, the AM realm which the user should log into.

Specify as many parameters as your custom login pages require:

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

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 chose it. In this case, you must ensure the custom login page *always* appends a `realm` parameter to the `goto` URL.
- The realm where the agent must log the user to has DNS aliases configured in AM. AM will log in the user to the realm whose DNS alias matches the incoming request URL. For example, an inbound request from the `http://marketplace.example.com` URL logs into the `marketplace` realm if the realm alias is set to `marketplace.example.com`.
- Users should always log in to the Top Level Realm.

Even if you specify the realm by default, this parameter can be overwritten by the custom login page if, for example, the user can chose the realm for authentication.

Default: `AMURL/am/UI/Login`

Property name	<code>com.sun.identity.agents.config.login.url</code> Introduced in Web Agent 4.x
Type	String Map
Bootstrap property	No
Required property	No
Restart required	No
AM console	Tab: AM Services  Title: AM Login URL



# Regular Expression Conditional Login Pattern

---

See [Regular Expression Conditional Login URL](#).

Property name	org.forgerock.agents.config.conditional.login.pattern Introduced in Web Agent 4.x
Type	String Map
Bootstrap property	No
Required property	No
Restart required	No
AM console	Tab: AM Services (From AM 7)  Title: Regular Expression Conditional Login Pattern

## Enable Custom Login Mode

---

Sets the login redirection mode, as follows:

- 0 : Disabled; default login redirection mode enabled.
- 1 : Enabled; non-OIDC compliant login flow, **standard** flow, where the agent does the following:
  - Tracks user authentication.
  - Converts the SSO token into an ID token at the end of the authentication flow.
  - Redirects the user to the originally requested resource.
  - The SSO token name is given by [Cookie Name](#).
- 2 : (For environments migrating from earlier versions of the agent) Enabled; non-OIDC compliant login flow, **non-standard** flow, where the agent does the following:
  - Does not track user authentication.
  - Redirects the user with a `goto` query parameter to the originally requested resource.
  - Configure this property with [Accept SSO Token](#), as described in [Login redirect configuration options](#) in the *User Guide*.

Default: 0

Property name	<code>org.forgerock.openam.agents.config.allow.custom.login</code> Introduced in Web Agent 5.5
Type	Integer
Bootstrap property	No
Required property	No
Restart required	No
AM console	Tab: AM Services (From AM 7) Title: Enable Custom Login Mode

## Logout redirect

### Disable Logout Redirection

---

During the logout flow and after logging out the user, this property specifies whether the agent should redirect the end user to another page. For example, to the landing page of the application, or to a login page:

`true` : Logout redirection is disabled - the agent does not perform the last redirection, and the web client is left on the logout page.

`false` : Logout redirection is enabled - the agent appends a `goto` parameter to the logout URL with the value of the [Logout Redirect URL](#).

Default: `true`

Property name	<code>com.forgerock.agents.config.logout.redirect.disable</code> Introduced in Web Agent 4.x
Type	Boolean: <code>true</code> returns true; all other strings return <code>false</code> .
Bootstrap property	No
Required property	No
Restart required	No

AM console	Tab: AM Services Title: Disable Logout Redirection
------------	---

## Logout URL List

One or more application logout URLs, such as `http://www.example.com/logout.html`. The agent triggers a logout flow when the end user accesses one of these pages. Therefore, these pages must be handled by your web server.

Configure with the [Logout Redirect URL](#) or [Agent Logout URL Regular Expression](#) properties.

Default: Empty

Property name	<code>com.sun.identity.agents.config.agent.logout.url</code> Introduced in Web Agent 4.x
Type	String Map
Bootstrap property	No
Required property	No
Restart required	No
AM console	Tab: AM Services Title: Logout URL List

## Enable Regex for Logout URL List

A flag to allow regular expressions in [Logout URL List](#).

Default: `false`

Property name	<code>org.forgerock.agents.config.logout.regex.enable</code> Introduced in Web Agent 4.x
Type	Boolean: <code>true</code> returns true; all other strings return <code>false</code> .
Bootstrap property	No

Required property	No
Restart required	No
AM console	Tab: AM Services (From AM 7) Title: Enable Regex for Logout URL List

## Enable Invalidate Logout Session

A flag for the agent to invalidate the end user session in AM, when it redirects a request to the logout URL:

- `true`: Invalidate the user session. Use when the value of Logout URL List is a page in your application, and your application **does not** handle the session invalidation process.
- `false`: Do not invalidate the user session. Use when the value of Logout URL List is:
  - A single SAML v2.0 logout page in AM
  - A page of an AM end user
  - A page in your application, and your application **does** handle the session invalidation process

Default: `true`

Property name	<code>org.forgerock.agents.config.logout.session.invalidate</code> Introduced in Web Agent 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
AM console	Tab: AM Services (From AM 7) Title: Enable Invalidate Logout Session

## Agent Logout URL Regular Expression

A Perl-compatible or ECMAScript-compatible (IIS) regular expression that matches logout URLs.

For example, to match URLs with `protectedA` or `protectedB` in the path and `op=logout` in the query string, use the following setting:

```
com.forgerock.agents.agent.logout.url.regex=(/protectedA\?|\protectedB\?/).(\&op=logout\&)(.*\|$\)
```

When this property is set, [Logout URL List](#) is ignored.

Default: Empty

Property name	<code>com.forgerock.agents.agent.logout.url.regex</code> Introduced in Web Agent 4.x
Type	String
Bootstrap property	No
Required property	No
Restart required	No
AM console	Tab: AM Services (From AM 7)  Title: Agent Logout URL Regular Expression

## AM Logout URL

The page to which the agent redirects the end user on log out. It can be a page in AM, such as `https://am.example.com:8443/am/UI/Logout?realm=/alpha`, or a page in the application.

The AM logout page invalidates the user session in AM, but pages in an application might not invalidate the user session in AM. See [Enable Invalidate Logout Session](#) for configuration options.

Default: `AM_URL/am/UI/Logout`

### IMPORTANT

By default, a realm is not included in the logout URL, and the user is redirected to the root realm on logout. Take care to include a realm if required.

Property name	<code>com.sun.identity.agents.config.logout.url</code> Introduced in Web Agent 4.x
---------------	---

Type	String Map
Bootstrap property	No
Required property	No
Restart required	No
AM console	Tab: AM Services Title: AM Logout URL

## Reset Cookies on Logout List

---

A list of cookies to be reset upon logout in the format: `name[=value][ ;Domain=value] .`

For example, `Cookie2=value;Domain=subdomain.domain.com` equates to:  
`com.sun.identity.agents.config.logout.cookie.reset[0]=Cookie2=value;Domain=subdomain.domain.com`

Default: Empty

Property name	<code>com.sun.identity.agents.config.logout.cookie.reset</code> Introduced in Web Agent 4.x
Type	String Map
Bootstrap property	No
Required property	No
Restart required	No
AM console	Tab: AM Services Title: Reset Cookies on Logout List

## Logout Redirect URL

---

The page to which the agent redirects the end user on log out if [Disable Logout Redirection](#) is `false`. Configure with [Logout URL List](#).

This URL must be available in your web server.

IMPORTANT

**IMPORTANT**

To ensure that the end user can access the logout page, add the URL to the [Not-Enforced URL List](#).

Default: Empty

Property name	com.sun.identity.agents.config.logout.redirect.url Introduced in Web Agent 4.x
Type	String
Bootstrap property	No
Required property	No
Restart required	No
AM console	Tab: AM Services Title: Logout Redirect URL

## Logs

### Local Audit Log Rotation Size

The maximum size in bytes of the local audit log files. The agent rotates audit log files when they reach this size, and stores rotated files with a timestamp.

Default: 52428800

Property name	com.sun.identity.agents.config.local.log.size Introduced in Web Agent 4.x
Type	Integer
Bootstrap property	Yes
Required property	No
Restart required	No

### Local Agent Debug File Name

The local file in which the agent writes debug log messages after startup.

During agent startup the location of the logs can be based on the container which is being used, or defined in the site configuration file for the server. For example, bootstrap logs for NGINX Plus Web Agent can be written to `/var/log/nginx/error.log`.

Default: `/web_agents/agent_type/instances/agent_nnn/logs/debug/debug.log`

Property name	<code>com.sun.identity.agents.config.local.logfile</code> Introduced in Web Agent 4.x
Type	String
Bootstrap property	Yes
Required property	No
Restart required	No

## Maximum Number of Debug Log Files

---

The maximum number of debug log files to store after log rotation.

If this property is `10`, the agent stores the current debug log file and up to 9 rotated log files. When logs are rotated again and a new log file is generated, the agent deletes the oldest of the stored log files and keeps the new log file.

To store no rotated logfiles, set [Agent Debug File Size](#) to zero.

Default: `0`, store all rotated log files

Property name	<code>com.forgerock.agents.config.max.num.log.files</code> Introduced in Web Agent 5.10.1
Type	Integer
Bootstrap property	Yes
Required property	No
Restart required	No

## Microsoft IIS server



## Show Password in HTTP Header

---

Set to `true` if encrypted password should be set in HTTP header `AUTH_PASSWORD`.

Default: `false`

Property name	<code>com.sun.identity.agents.config.iis.password.header</code> Introduced in Web Agent 4.x
Type	Boolean: <code>true</code> returns true; all other strings return <code>false</code> .
Bootstrap property	No
Required property	No
Restart required	No
AM console	Tab: Advanced  Title: Show Password in HTTP Header

## Logon and Impersonation

---

When `true`, the agent does Windows Logon and User Impersonation.

Default: `false`

Property name	<code>com.sun.identity.agents.config.iis.logonuser</code> Introduced in Web Agent 4.x
Type	Boolean: <code>true</code> returns true; all other strings return <code>false</code> .
Bootstrap property	No
Required property	No
Restart required	No
AM console	Tab: Advanced  Title: Logon and Impersonation

## Remove IIS HTTP Server Header

---

When `true`, the IIS agent will remove the Server header

Default: `false`

Property name	<code>org.forgerock.agents.config.iis.headers.server.disable</code> Introduced in Web Agent 2023.2
Type	Boolean: <code>true</code> returns true; all other strings return <code>false</code> .
Bootstrap property	Yes
Required property	No
Restart required	No

## Replay Password Key

---

DES key for decrypting the basic authentication password in the session.

Default: Empty

Property name	<code>com.sun.identity.agents.config.replaypasswd.key</code> Introduced in Web Agent 4.x
Type	String
Bootstrap property	No
Required property	No
Restart required	No
AM console	Tab: Advanced  Title: Replay Password Key

## Miscellaneous

## TCP Receive Timeout

---

The number of seconds to wait for a response from AM before timing out and dropping the connection. Applies to TCP receive operations.

Default: 4

Property name	<code>com.sun.identity.agents.config.receive.timeout</code> Introduced in Web Agent 5.5
Type	Integer
Bootstrap property	Yes
Required property	No
Restart required	No

## AM Connection URL

---

A space-delimited list of AM URLs to which the agent connects. Set this property to the URL of the load balancer in front of the AM instances (or load balancers, in case of disaster-recovery configurations).

When the agent cannot connect to the first URL in the list, it automatically connects to the next available URL. The agent stays connected to the new URL until the URL fails, or the agent is restarted.

Default: `AM_URL/am/`

Property name	<code>com.sun.identity.agents.config.naming.url</code> Introduced in Web Agent 4.x
Type	String List
Bootstrap property	Yes
Required property	No
Restart required	No

## Connection Timeout

---

The number of seconds to wait for a connection to AM before timing out and cancelling the connection. Applies to TCP connect operations.

Default: 4

Property name	<code>com.sun.identity.agents.config.connect.timeout</code> Introduced in Web Agent 5.5
Type	Integer
Bootstrap property	Yes
Required property	No
Restart required	No

## Security Protocol List

---

A space-separated list of security protocols preceded by a dash (-) that are **not** used when connecting to AM. The following protocols are supported:

- SSLv3
- TLSv1
- TLSv1.1
- TLSv1.2 (Enabled)
- TLSv1.3 (Enabled)

SSLv2 is always disabled, regardless of the setting.

This property is relevant to all Web Agents using OpenSSL libraries.

To change the default value, set an environment variable, `AM_SSL_OPTIONS`.

Default: `-SSLv3 -TLSv1 -TLSv1.1`

Property name	<code>org.forgerock.agents.config.tls</code> Introduced in Web Agent 4.x
Type	String
Bootstrap property	Yes
Required property	No
Restart required	No

# Use Built-in Apache HTTPD Authentication Directives

---

A regular expression pattern to specify which not-enforced URLs can use built-in Apache authentication directives, such as `AuthName`, `FilesMatch`, and `Require`, for basic authentication.

Requests with not-enforced URLs that match the expression can use built-in Apache authentication directives.

Default: No requests can use built-in Apache authentication directives.

Property name	<code>com.forgerock.agents.no.remoteuser.module.compatibility</code> Introduced in Web Agent 5.9
Type	Unused
Bootstrap property	No
Required property	No
Restart required	No
AM console	Tab: Advanced (From AM 7.2)  Title: Use Built-in Apache HTTPD Authentication Directives

## Not-enforced

## Ignore Path Info in Not-Enforced URLs

---

When `true`, strip path info and query from the request URL before comparing it with the URLs in [Not-Enforced URL List](#) for those URLs containing a wildcard character. This prevents a user from accessing `http://host/index.html` by requesting `http://host/index.html/hack.gif` when the not-enforced list includes `http://host/*.gif`.

### NOTE

The NGINX Plus web agent does not support this setting.

Default: `true`

Property name	<code>com.sun.identity.agents.config.ignore.path.info.for.not.enforced.list</code> Introduced in Web Agent 4.x
Type	Boolean: <code>true</code> returns true; all other strings return <code>false</code> .
Bootstrap property	No
Required property	No
Restart required	No
AM console	Tab: Application  Title: Ignore Path Info in Not-Enforced URLs

## Regular Expressions for Not-Enforced URLs

### IMPORTANT

Regular expressions are evaluated differently by different engines. When you use regular expressions in not-enforced lists, make sure that the expressions are evaluated in the way you expect. Double check that the correct URLs are enforced and not enforced.

When `true`, allow the use of Perl-compatible or ECMAScript-compatible (IIS) regular expressions in [Not-Enforced URL List](#) settings.

Default: `false`

Property name	<code>com.forgerock.agents.notenforced.url.regex.enable</code> Introduced in Web Agent 4.x
Type	Boolean: <code>true</code> returns true; all other strings return <code>false</code> .
Bootstrap property	No
Required property	No
Restart required	No

AM console	Tab: Application (From AM 7)  Title: Regular Expressions for Not-Enforced URLs
------------	--

## Enable Regular Expressions for Not-Enforced IPs

### IMPORTANT

Regular expressions are evaluated differently by different engines. When you use regular expressions in not-enforced lists, make sure that the expressions are evaluated in the way you expect. Double check that the correct URLs are enforced and not enforced.

A flag to enable Perl-compatible regular expressions or ECMAScript-compatible (IIS) in Not-Enforced URL from IP Processing List.

Default: false

Property name	<code>org.forgerock.agents.config.notenforced.ext.regex.enable</code> Introduced in Web Agent 4.x
Type	Boolean: true returns true; all other strings return false.
Bootstrap property	No
Required property	No
Restart required	No
AM console	Tab: Application (From AM 7)  Title: Enable Regular Expressions for Not-Enforced IPs

## Not-Enforced Fallback Mode

A flag to specify whether the agent allows traffic to resources specified in the not-enforced lists when AM is not available:

- `true` : While AM is unavailable, the agent reads the cached agent profile configuration until it expires. After the cache expires, reads the local configuration file ( `agent.conf` ). If not-enforced properties are configured in `agent.conf` , the

agent allows access to the not-enforced resources. However, response attributes for not-enforced resources are not available until AM is accessible.

- `false` : When AM is unavailable, the web agent prevents access to all resources, including any not-enforced resources.

Configure the following properties in `agent.conf` , even if the agent profile is in centralized configuration:

- `com.forgerock.agents.config.fallback.mode = true`
- `com.sun.identity.agents.config.notenforced.url.attributes.enable = true`
- `com.sun.identity.agents.config.notenforced.url.invert = false`
- `com.sun.identity.agents.config.notenforced.url[0] = http://agenttest.example.com/index.html`

Default: `false`

Property name	<code>com.forgerock.agents.config.fallback.mode</code> Introduced in Web Agent 4.x
Type	Boolean: <code>true</code> returns true; all other strings return <code>false</code> .
Bootstrap property	Yes
Required property	No
Restart required	No
AM console	Tab: Application  Title: Not-Enforced Fallback Mode

## Client IP Validation

---

When `true` , validate that the subsequent browser requests come from the same IP address that the SSO token is initially issued against.

Default: `false`

Property name	<code>com.sun.identity.agents.config.client.ip.validation.enable</code> Introduced in Web Agent 4.x
---------------	--



Type	Boolean: true returns true; all other strings return false .
Bootstrap property	No
Required property	No
Restart required	No
AM console	Tab: Application Title: Client IP Validation

## Invert Not-Enforced URLs

---

When `true`, enforce policy for the URLs and patterns specified in [Not-Enforced URL List](#), instead of allowing access to them without authentication. Consider the following points when configuring this property:

- If [Not-Enforced URL List](#) is empty, all URLs are enforced
- At least one URL must be enforced. To allow access to any URL without authentication, consider disabling the agent.

Default: `false`

Property name	<code>com.sun.identity.agents.config.notenforced.url.invert</code> Introduced in Web Agent 4.x
Type	Boolean: true returns true; all other strings return false .
Bootstrap property	No
Required property	No
Restart required	No
AM console	Tab: Application Title: Invert Not-Enforced URLs

## Not-Enforced URL List

---

A space-delimited list of URIs for which the agent does not enforce authentication or request policy evaluations.

For information about configuring not-enforced lists, see [Not-enforced rules](#) in the *User Guide*.

Default: Empty

Property name	<code>com.sun.identity.agents.config.notenforced.url</code> Introduced in Web Agent 4.x
Type	String Map
Bootstrap property	No
Required property	No
Restart required	No
AM console	Tab: Application Title: Not-Enforced URL List

## Fetch Attributes for Not-Enforced URLs

When `true`, the agent fetches profile, response, and session attributes that are mapped by policy evaluations, and forwards these attributes to not-enforced URLs.

Default: `false`

Property name	<code>com.sun.identity.agents.config.notenforced.url.attributes.enable</code> Introduced in Web Agent 4.x
Type	Boolean: <code>true</code> returns true; all other strings return <code>false</code> .
Bootstrap property	No
Required property	No
Restart required	No
AM console	Tab: Application Title: Fetch Attributes for Not-Enforced URLs

## Not-Enforced IP List

---

A space-delimited list of IP addresses or network CIDR notation addresses for which the agent does not enforce authentication or request policy evaluations.

Supported values are IPV4 and IPV6 addresses, IPV4 and IPV6 ranges of addresses delimited by the - character, and network ranges specified in CIDR notation.

This property can apply to methods. The following example does not enforce GET requests in the specified IP range:

```
com.sun.identity.agents.config.notenforced.ip[1,GET]=iprange
```

For information about configuring not-enforced lists, see [Not-enforced rules](#) in the *User Guide*.

Default: Empty

Property name	com.sun.identity.agents.config.notenforced.ip Introduced in Web Agent 4.x
Type	String Map
Bootstrap property	No
Required property	No
Restart required	No
AM console	Tab: Application  Title: Not-Enforced IP List

## Not-Enforced URL from IP Processing List

---

A space-delimited list of IP addresses or network CIDR notation addresses for which the agent does not enforce authentication or request policy evaluations.

When | and a list of IP addresses is used, the request is not enforced if it comes from one of the IP ranges AND it is asking for one of the URLs.

In the following example, the agent does not enforce HTTP requests from the IP addresses 192.6.8.0/24 to any file in /public, or any files or directories that start with the string login in the directory /free\_access URI:

```
org.forgerock.agents.config.notenforced.ipurl[1]=192.6.8.0/24|http://www.example.com:8080/public/* /free_access/login
```

Default: Empty

Property name	<code>org.forgerock.agents.config.notenforced.ipurl</code> Introduced in Web Agent 4.x
Type	String Map
Bootstrap property	No
Required property	No
Restart required	No
AM console	Tab: Application (From AM 7)  Title: Not-Enforced URL from IP Processing List

## POST data preservation

### Enable POST Data Preservation

---

A flag to enable HTTP POST data preservation.

Default: `false`

Property name	<code>com.sun.identity.agents.config.postdata.preserve.enable</code> Introduced in Web Agent 4.x
Type	Boolean: <code>true</code> returns true; all other strings return <code>false</code> .
Bootstrap property	No
Required property	No
Restart required	No
AM console	Tab: Advanced  Title: Enable POST Data Preservation

### POST Data Entries Cache Period

---

Number of minutes before expiry of the Post Data Preservation cache.

Consider setting Profile Attributes Cookie Maxage to at least the value of this property.

Default: 10

Property name	<code>com.sun.identity.agents.config.postcache.entry.lifetime</code> Introduced in Web Agent 4.x
Type	Integer
Bootstrap property	No
Required property	No
Restart required	No
AM console	Tab: Advanced  Title: POST Data Entries Cache Period

## POST Data Storage Directory

---

The local directory where the agent writes preserved POST data while requesting authorization from AM.

Default: `/web_agents/agent_type/log`

Property name	<code>org.forgerock.agents.config.postdata.preserve.dir</code> Introduced in Web Agent 4.x
Type	String
Bootstrap property	Yes
Required property	No
Restart required	No
AM console	Tab: Advanced  Title: POST Data Storage Directory

## URLs Ignored by the POST Data Inspector

A list of URLs that are not be processed by the agent POST data inspector. Other modules on the same server can access the POST data directly.

The following example uses wildcards to add a file named `postreader.jsp` in the root of any protected website to the list of URLs that will not have their POST data inspected:

```
org.forgerock.agents.config.skip.post.url[0]=http*:///postreader.jsp
```

### NOTE

URLs added to this property should also be added to [Not-Enforced URL List](#).

Default: Empty

Property name	<code>org.forgerock.agents.config.skip.post.url</code> Introduced in Web Agent 4.x
Type	String Map
Bootstrap property	No
Required property	No
Restart required	No
AM console	Tab: Advanced (From AM 7)  Title: URLs Ignored by the POST Data Inspector

## Submit POST Data using JavaScript

When `true`, preserved POST data is resubmitted to the destination server after authentication by using JavaScript.

Default: `false`

Property name	<code>org.forgerock.agents.pdp.javascript.repost</code> Introduced in Web Agent 4.x
Type	Boolean: <code>true</code> returns true; all other strings return <code>false</code> .
Bootstrap property	No

Required property	No
Restart required	No
AM console	Tab: Advanced (From AM 7) Title: Submit POST Data using JavaScript

## Policy client service

## User ID Parameter

The User ID passed in the session from AM to the REMOTE\_USER server variable.

Default: UserToken

Property name	com.sun.identity.agents.config.userid.param Introduced in Web Agent 4.x
Type	String
Bootstrap property	No
Required property	No
Restart required	No
AM console	Tab: AM Services Title: User ID Parameter

## Policy Cache Polling Period

Polling interval in minutes during which an entry remains valid after being added to the agent cache.

Default: 3

Property name	com.sun.identity.agents.config.policy.cache.polling.interval Introduced in Web Agent 4.x
Type	Integer

Bootstrap property	No
Required property	No
Restart required	No
AM console	Tab: AM Services Title: Policy Cache Polling Period

## Policy Clock Skew

---

Number of seconds to allow for time difference between agent system and AM. Clock skew in seconds = AgentTime - AMServerTime.

Use this property to adjust for small time differences encountered despite use of a time-synchronization service. When this property is not set and agent time is greater than AM server time, the agent can make policy calls to the AM server before the policy subject cache has expired, or you can see infinite redirection occur.

Default: 0

Property name	com.sun.identity.agents.config.policy.clock.skew Introduced in Web Agent 4.x
Type	Integer
Bootstrap property	No
Required property	No
Restart required	No
AM console	Tab: AM Services Title: Policy Clock Skew

## Policy Evaluation Realm

---

In AM 6.5, this property was named Realm.

The realm where AM evaluates polices for policy decision requests from the agent. This property is recognized by AM, not the agent.



The policy set configured by Policy\_Set must exist in the realm configured by this property. Otherwise, policy evaluation produces DENY results without writing warnings to the logs.

The default policy set exists only in the top-level realm. If you are using a different realm for policy evaluation, do one of the following:

- Create the `iPlanetAMWebAgentService` policy set in that realm.
- Create a different policy set in that realm, and configure Policy\_Set to use it.

Default: (/) top-level realm

Property name	<code>org.forgerock.openam.agents.config.policy.evaluation.realm</code> Introduced in Web Agent 4.x
Type	String
Bootstrap property	Yes
Required property	No
Restart required	No
AM console	Tab: AM Services Title: Policy Evaluation Realm

## Fetch Policies From The Root Resource

---

When `true`, the agent caches the policy decision of the resource and all resources from the root of the resource down.

For example, if the resource is `http://host/a/b/c`, then the root of the resource is `http://host/`.

Use this property when a client is expected to access multiple resources on the same path. However, caching can be expensive if very many policies are defined for the root resource.

Default: `false`

Property name	<code>com.sun.identity.agents.config.fetch.from.root.resource</code> Introduced in Web Agent 4.x
---------------	---

Type	Boolean: true returns true; all other strings return false.
Bootstrap property	No
Required property	No
Restart required	No
AM console	Tab: AM Services Title: Fetch Policies From The Root Resource

## Enable Retrieve Client Hostname

---

When true, get the client hostname through DNS reverse lookup for use in policy evaluation. This setting can impact performance.

Default: false

Property name	com.sun.identity.agents.config.get.client.hostname Introduced in Web Agent 4.x
Type	Boolean: true returns true; all other strings return false.
Bootstrap property	No
Required property	No
Restart required	No
AM console	Tab: AM Services Title: Enable Retrieve Client Hostname

## SSO Cache Polling Period

---

Polling interval in minutes during which an SSO entry remains valid after being added to the agent cache.

Default: 3

Property name	<code>com.sun.identity.agents.config.sso.cache.polling.interval</code> Introduced in Web Agent 4.x
Type	Integer
Bootstrap property	No
Required property	No
Restart required	No
AM console	Tab: AM Services  Title: SSO Cache Polling Period

## User ID Parameter Type

---

Fetch user ID from SESSION or LDAP attributes.

Default: SESSION

Property name	<code>com.sun.identity.agents.config.userid.param.type</code> Introduced in Web Agent 4.x
Type	String
Bootstrap property	No
Required property	No
Restart required	No
AM console	Tab: AM Services  Title: User ID Parameter Type

## Policy Set

---

In AM 6.5, this property was named Application.

The name of the policy set where AM evaluates polices for policy decision requests from the agent.

By default, AM evaluates policies in `iPlanetAMWebAgentService`. Set this property to cause AM to use a different policy set. This property is recognized by AM, not the agent.

The policy set configured by this property must exist in the realm configured by [Policy Evaluation Realm](#). Otherwise, policy evaluation produces DENY results without writing warnings to the logs.

The default policy set exists only in the top-level realm. If you are using a different realm for policy evaluation, do one of the following:

- Create the `iPlanetAMWebAgentService` policy set in that realm.
- Create a different policy set in that realm, and configure this property to use it.

Default: `iPlanetAMWebAgentService`

Property name	<code>org.forgerock.openam.agents.config.policy.evaluation.application</code> Introduced in Web Agent 4.x
Type	String
Bootstrap property	Yes
Required property	No
Restart required	No
AM console	Tab: AM Services Title: Policy Set

## Profile

### Accept SSO token cookie (deprecated)

Use [Accept SSO Token](#) instead of this property.

Property name	<code>com.forgerock.agents.accept.ipdp.cookie</code> Introduced in Web Agent 5.7
Type	Integer
Bootstrap property	No
Required property	No

Restart required	No
AM console	Tab: Global Title: Accept SSO token cookie (deprecated)

## Agent Profile ID Allow List

---

A comma-separated list of profile IDs that the agent considers as valid values for the `aud` claim. This claim is represented in the ID token containing the end user's session.

When several agents are configured with different agent profiles to protect the same application, set this property to a list of the agent profiles that are protecting the same application.

With the following setting, the agent considers `agentprofile1` and `agentprofile2` to be valid, and does not validate them:

```
com.forgerock.agents.jwt.aud.whitelist=agentprofile1,agentprofile2
```

Default: Empty

Property name	<code>com.forgerock.agents.jwt.aud.whitelist</code> Introduced in Web Agent 5.7
Type	String
Bootstrap property	No
Required property	No
Restart required	No
AM console	Tab: Global Title: Agent Profile ID Allow List

## Web Socket Connection Interval

---

The time in minutes before WebSockets to AM are killed and reopened. Use this property to balance the distribution of connections across the AM servers on the site.

Default: 30

Property name	<code>org.forgerock.openam.agents.config.balance.websocket.connection.interval.in.minutes</code> Introduced in Web Agent 4.x
Type	Integer
Bootstrap property	Yes
Required property	No
Restart required	No
AM console	Tab: Global  Title: Web Socket Connection Interval

## Enable Notifications of Agent Configuration Change

---

A flag to specify whether AM sends a notification to the agent to reread the agent profile after a change to a hot-swappable property. This property applies only when you store the agent profile in AM's configuration data store.

Default: true

Property name	<code>com.sun.identity.agents.config.change.notification.enable</code> Introduced in Web Agent 4.x
Type	Unused
Bootstrap property	No
Required property	No
Restart required	No
AM console	Tab: Global  Title: Enable Notifications of Agent Configuration Change

## Configuration Reload Interval

---

Time in minutes after which the agent fetches the configuration from AM. Used if notifications are disabled.

Default: 60

Property name	<code>com.sun.identity.agents.config.polling.interval</code> Introduced in Web Agent 4.x
Type	Integer
Bootstrap property	No
Required property	No
Restart required	No
AM console	Tab: Global  Title: Configuration Reload Interval

## Agent Root URL for CDSSO

---

The agent root URLs for CDSSO. The valid value is in the format `protocol://hostname:port/`, where `protocol` represents the protocol used, such as `http` or `https`, `hostname` represents the host name of the system where the agent resides, and `port` represents the port number on which the agent is installed. The slash following the port number is required.

If your agent system has virtual host names, add URLs with the virtual host names to this list. AM checks that the `goto` URLs match one of the agent root URLs for CDSSO.

Default: `agent-root-URL`

Property name	<code>sunIdentityServerDeviceKeyValue</code> Introduced in Web Agent 4.x
Type	Unused
Bootstrap property	No
Required property	No
Restart required	No

AM console	Tab: Global  Title: Agent Root URL for CDSSO
------------	--

## Disable Audience Claim Validation

The claims to validate in the ID token containing the end user's session:

- 0 : Validate the aud and nonce claim.
- 1 : Validate the nonce claim; don't validate the aud claim.

During an authentication request, AM creates an ID token that contains, among others, the end user's session, and the aud claim. The aud claim is set to the agent profile of the agent that made the request. When AM returns the ID token to the end user's user-agent, it appends a nonce parameter to the request, which is a one-time-usable random string that is understood by both AM and the agent that made the authentication request.

When the agent receives a request to access a protected resource, the agent checks that the audience (the aud claim) of the ID token and the value of the nonce are appropriate. For example, it checks that the value of the aud claim is the name of its own agent profile.

In environments where several agents protect the same application, this validation poses a problem; even if the ID token is valid and contains a valid session, an agent cannot validate a ID token created for a different agent because the audience would not match. Therefore, the agent redirects the end user to authenticate again.

### TIP

For security reasons, agents should validate as many claims in the ID token as possible.

Default: 0

Property name	com.forgerock.agents.jwt.aud.disable Introduced in Web Agent 5.7
Type	Integer
Bootstrap property	No
Required property	No
Restart required	No



AM console	Tab: Global  Title: Disable Audience Claim Validation
------------	---

## JWT Cookie Name

The name of the cookie that holds the OpenID Connect ID token on the user's browser. Before changing the name of this cookie, consider the following points:

- The cookie is only used by the agent and is never presented to AM.
- The cookie name must be unique across the set of cookies the user's browser receives, since some browsers behave in unexpected ways when receiving several cookies with the same name. For example, you should not set the session ID token cookie name to `iPlanetDirectoryPro`, which is the default name of AM's session cookie.

Default: `am-auth-jwt`

Property name	<code>org.forgerock.openam.agents.config.jwt.name</code> Introduced in Web Agent 4.x
Type	String
Bootstrap property	Yes
Required property	No
Restart required	No
AM console	Tab: Global  Title: JWT Cookie Name

## Password

The agent password used when creating the password file and when installing the agent.

If you change the password, manually update the password in [Agent Profile Password](#).

Property name	<code>password</code> Introduced in Web Agent 4.x
Type	Unused

Bootstrap property	No
Required property	No
Restart required	No

## Location of Agent Configuration Repository

---

The management mode for the agent configuration:

- `centralized`: The configuration is managed through AM.
- `local`: The configuration is managed locally in the agent configuration file. In local configuration, you cannot manage the agent configuration through the AM console.

Default: `centralized`

Property name	<code>com.sun.identity.agents.config.repository.location</code> Introduced in Web Agent 4.x
Type	String
Bootstrap property	Yes
Required property	No
Restart required	No
AM console	Tab: Global  Title: Location of Agent Configuration Repository

## Retain Session Cache After Configuration Change

---

Use this property to manage how the session cache is used after a change to the agent configuration:

- `0`: Purge the session cache, and re-read the user session data.
- `1`: Do not purge the session cache, and do not re-read the user session data. Use this value to prevent the agent from flooding AM instances with requests, when the agent configuration changes regularly, and the changes do not affect the agent authorisation decisions.

Default: 0

Property name	<code>com.forgerock.agents.session.cache.eventually.consistent</code> Introduced in Web Agent 5.9
Type	Boolean: true returns true; all other strings return false.
Bootstrap property	No
Required property	No
Restart required	No
AM console	Tab: Advanced (From AM 7.2)  Title: Retain Session Cache After Configuration Change

## Agent Deployment URI Prefix

Overrides the request URL given by the agent, when the agent is configured behind a load balancer or proxy. Use this property when the protocol, hostname, or port of the load balancer or proxy differ from those of the agent.

At least one of the following properties must be enabled:

- [Enable Override Request URL Port](#)
- [Enable Override Request URL Protocol](#)
- [Enable Override Request URL Host](#)

Use these properties only if you are not using x-forwarded headers from the load balancer or proxy to override the agent's protocol, hostname, and port values.

Default: agent-root-URL

Property name	<code>com.sun.identity.agents.config.agenturi.prefix</code> Introduced in Web Agent 4.x
Type	String
Bootstrap property	No
Required property	No

Restart required	No
AM console	Tab: Global Title: Agent Deployment URI Prefix

## Use Cached Configuration After Update

### IMPORTANT

Use this property only on recommendation from ForgeRock support, to reduce unnecessary concurrent authentication requests to AM.

When the agent receives requests after the agent config has been updated in AM, a single request thread calls AM to download the new configuration. This property manages the response for the concurrent request threads, as follows:

- `false` : Concurrent request threads wait for the time specified by [TCP Receive Timeout](#) for the retrieving request thread to complete, and then they use the new configuration.
- `true` : Concurrent request threads that can use the out-of-date, cached configuration do so, without waiting for the new configuration.

Set this property according to the value of [Location of Agent Configuration Repository](#):

- `local` : In the local bootstrap file.
- `central` : In the AM console. The value in the AM console takes precedence over the local bootstrap file.

Default: `false`

Property name	<code>com.forgerock.agents.config.use.during.update</code> Introduced in Web Agent 4.x
Type	Boolean: <code>true</code> returns true; all other strings return <code>false</code> .
Bootstrap property	Yes
Required property	No
Restart required	No

AM console	Tab: Advanced  Title: Use Cached Configuration After Update
------------	---

## Enable Notifications

---

When `true`, AM can sent notifications to the agent to:

- Refresh the session cache when a session times out or a client logs out from AM.
- Refresh the policy cache when the administrator changes a policy.

Default: `true`

Property name	<code>com.sun.identity.agents.config.notification.enable</code> Introduced in Web Agent 4.x
Type	Boolean: <code>true</code> returns true; all other strings return <code>false</code> .
Bootstrap property	Yes
Required property	No
Restart required	No
AM console	Tab: Global  Title: Enable Notifications

## Group

---

Status of the agent configuration.

Property name	<code>group</code> Introduced in Web Agent 4.x
Type	Unused
Bootstrap property	No
Required property	No

Restart required	No
------------------	----

## URL handling

### Encode Special Characters in URLs

---

When `true`, encode the URL a URL with special characters before doing policy evaluation.

Default: `false`

Property name	<code>com.sun.identity.agents.config.encode.url.special.chars.enable</code> Introduced in Web Agent 4.x
Type	Boolean: <code>true</code> returns true; all other strings return <code>false</code> .
Bootstrap property	No
Required property	No
Restart required	No
AM console	Tab: Miscellaneous  Title: Encode Special Characters in URLs

### Enable URL Comparison Case Sensitivity Check

---

When `true`, enforce case insensitivity in policy evaluation and not-enforced URL evaluation.

Default: `true`

Property name	<code>com.sun.identity.agents.config.url.comparison.case.ignore</code> Introduced in Web Agent 4.x
Type	Boolean: <code>true</code> returns true; all other strings return <code>false</code> .

Bootstrap property	No
Required property	No
Restart required	No
AM console	Tab: Miscellaneous  Title: Enable URL Comparison Case Sensitivity Check

## Invalid URL Regular Expression

A Perl-compatible or ECMAScript-compatible (IIS) regular expression to parse valid request URLs. The agent rejects requests to invalid URLs with HTTP 403 Forbidden status without further processing.

For example, to filter out URLs containing a list of characters and words such as ... %00-%1f, %7f-%ff, %25, %2B, %2C, %7E, configure the following regular expression:

```
com.forgerock.agents.agent.invalid.url.regex=http[s]?:\//[^/]+\/(?i)(?!\\|
[?]\\//|\.\.\/|[?]\\.\.|\//\|\.\.|\~|[?]%2d|%20|[?][0-1][0-9a-f]|%[7-9a-f][0-9a-
f]|[?]%25)[?]?.
```

Default: Empty

Property name	com.forgerock.agents.agent.invalid.url.regex Introduced in Web Agent 4.x
Type	String
Bootstrap property	No
Required property	No
Restart required	No
AM console	Tab: Miscellaneous (From AM 7)  Title: Invalid URL Regular Expression

---

Copyright © 2010-2023 ForgeRock, all rights reserved.